ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ
ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ
DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

КЕРИМОВ КОМИЛ ФИКРАТОВИЧ

ЭЛЕКТРОН РЕСУРСЛАРНИ АХБОРОТ ХАВФСИЗЛИГИ ТАҲДИДЛАРИДАН ҲИМОЯСИНИ ТАЪМИНЛАШНИНГ МОСЛАШУВЧАН МОДЕЛЛАРИ ВА УСУЛЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ ДОКТОРИ (DSc)
ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

Тошкент – 2020

УДК 004.056+004.93

Докторлик (DSc) диссертацияси автореферати мундарижаси

Оглавление автореферата докторской (DSc) диссертации

Contents of the abstract of Doctoral (DSc) dissertation

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

КЕРИМОВ КОМИЛ ФИКРАТОВИЧ

ЭЛЕКТРОН РЕСУРСЛАРНИ АХБОРОТ ХАВФСИЗЛИГИ ТАҲДИДЛАРИДАН ҲИМОЯСИНИ ТАЪМИНЛАШНИНГ МОСЛАШУВЧАН МОДЕЛЛАРИ ВА УСУЛЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент – 2020

Техника фанлари доктори (DSc) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2018.4.DSc/T243 рақам билан рўйхатга олинган.

Диссертация Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.tuit.uz) ва «Ziyonet» ахборот-таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий маслаҳатчи:	**Ҳамдамов Рустам Ҳамдамович** техника фанлари доктори, профессор
Расмий оппонентлар:	**Бекмуратов Тулкун Файзиевич** техника фанлари доктори, профессор, академик
	Мусаев Мухаммаджон Махмудович техника фанлари доктори, профессор
	Опанасенко Владимир Николаевич техника фанлари доктори, профессор
Етакчи ташкилот:	**Мирзо Улуғбек номидаги Ўзбекистон миллий университети**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.1.07.01 рақамли Илмий кенгашнинг 2020 йил «30» декабрь да соат 10:00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университетининг Ахборот-ресурс марказида танишиш мумкин (158 рақам билан рўйхатга олинган). Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43).

Диссертация автореферати 2020 йил «18» декабрь куни тарқатилди.
(2020 йил «17» декабрдаги 43 рақамли реестр баённомаси)

Ш.Х.Фозилов
Илмий даражалар берувчи илмий кенгаш раиси ўринбосари, т.ф.д., профессор

Ф.М.Нуралиев
Илмий даражалар берувчи илмий кенгаш илмий котиби, т.ф.д., доцент

С.К. Ганиев
Илмий даражалар берувчи илмий кенгаш ҳузуридаги илмий семинар раиси т.ф.д., профессор

КИРИШ (докторлик диссертацияси автореферати (DSc))

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда электрон ресурслар ва веб-иловалар хавфсизлигини таъминлашга алоҳида эътибор қаратилмоқда. Электрон ресурсларни ҳимоя қилиш тизимларини ишлаб чиқиш, шунингдек уларни давлат ташкилотлари (вазирликлар, идоралар, йирик компаниялар), банклар (давлат ва хусусий), электрон тижорат (онлайн-дўконлар, тўлов тизимлари), турли саноат ва тижорат корхоналари, ахборот ва таълим ресурслари (масофавий ўқитиш, онлайн кутубхоналар) ва бошқа йўналишлар учун автоматлаштирилган тизимларни ҳимоя қилиш учун қўллаш, корхоналарнинг ўзи учун ҳам, умуман давлат учун ҳам катта аҳамиятга ега. Бугунги кунда электрон ресурсларни ҳимоя қилишнинг турли усуллари, хусусан, шаблонларга асосланган, аномалия таъсир қилиш ва хулқ-атвор таҳлилига асосланган усуллар ишлаб чиқилган ва тадқиқ қилинган. Электрон ресурсларни ҳимоя қилиш муаммоларига АҚШ, Жанубий Корея, Украина, Япония, Россия Федерацияси, Ҳиндистон ва бошқа мамлакатларда катта эътибор қаратилмоқда.

Жаҳонда электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишни таъминлаш учун фойдаланиладиган моделлар ва усулларни ишлаб чиқишга қаратилган илмий тадқиқотлар олиб борилмоқда. Шунга қарамай, мавжуд электрон ресурсларни ҳимоя қилиш тизимлари фақат базада мавжуд бўлган таҳдидларни аниқлаш ва ҳимоя қилишга имкон берувчи шаблонлар усулига асосланган. Таҳдидларни аниқлаш ва ажратишда бир қатор муаммолар мавжуд: мавжуд усулларининг индивидуал эмпирик хусусиятларга боғлиқлиги, бу эса тизимнинг кўплаб нотўғри сигналлар беришига олиб келади; маълум бўлган таҳдидларнинг тор доираси; номаълум параметрлар билан ифодаланган янги таҳдидларни аниқлашнинг мумкин эмаслиги. Ушбу йўналишда мослашувчан усулларини, моделларини ишлаб чиқиш, хавфсизлик кўрсаткичларининг сабаб-оқибат таҳлилини яратиш керак. Шунингдек, фойдаланиш учун қулай, сервер майдонида ўрнатилиши осон бўлган ҳамда самарали ишловчи дастурий таъминотни ишлаб чиқиш зарур бўлади.

Республикамизда кўпгина фаолият соҳаларида ахборот технологияларини жорий этишга, шу жумладан, ахборотни ҳимоя қилиш моделлари ва усулларини ишлаб чиқишда илмий тадқиқотлар ўтказишга алоҳида эътибор қаратилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича ҳаракатлар стратегиясида «... иқтисодиёт, ижтимоий соҳа, бошқарув тизимига ахборот-коммуникация технологияларини жорий этиш»[1] каби вазифалар белгиланган. Ушбу вазифаларни бажариш учун синалли ва хулқ-атвор таҳлили асосида электрон ресурсларни ҳимоя қилишнинг мослашувчан моделлари ва усулларини ишлаб чиқиш муҳим аҳамиятга ега.

---

[1] Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги Фармони.

Ушбу диссертация тадқиқоти маълум даражада Ўзбекистон Республикаси Президентининг 2018 йил 19 февралдаги УФ-5349-сонли "Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида" фармонида, Ўзбекистон Республикаси Президентининг 2017 йил 29 августдаги ПҚ-3245 "Ахборот ва коммуникация технологиялари соҳасида лойиҳаларни бошқариш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида", Ўзбекистон Республикаси Президентининг 2018 йил 21 ноябрдаги ПҚ-4024-сонли "Ахборот технологиялари ва коммуникацияларини жорий этиш устидан назорат тизимини такомиллаштириш чора-тадбирлари тўғрисида" қарорларидаги, Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2018 йилда 5 сентябрдаги " Интернет глобал тармоғида ахборот хавфсизлигини яхшилаш чора-тадбирлари тўғрисида" № ВМҚ-707-сонли қарорида белгиланган вазифаларни бажаришга хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги. Ушбу тадқиқот республикада фан ва техника тараққиётининг IV "Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш" устувор йўналишларига мувофиқ амалга оширилди.

Диссертация мавзуси бўйича хорижий илмий-тадқиқотлар шарҳи.

Электрон ресурсларда ахборот хавфсизлиги таҳдидларини ҳимоя қилиш ва аниқлаш моделларини ишлаб чиқишга йўналтирилган илмий тадқиқотлар дунёнинг етакчи илмий марказларида ва олий ўқув юртларида, шу жумладан, IBM Cyber Security Center of Excellence, Open Web Application Security Project, Information Security Research Association, SRI internation, Norwegian University of Science and Technology (Норвегия), University of South Wales, The University of Oxford (Буюк Британия), New Hampshire University (АҚШ), Seoul National University (Жанубий Корея), Asahi Kasei Microsystems (Япония), Москва давлат университети (Россия Федерацияси), "Техник ёрдам маркази" ДУКда (Ўзбекистон) олиб борилади.

Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари ва моделлари бўйича дунёда олиб борилган тадқиқотлар натижасида бир қатор илмий натижаларга эришилди, жумладан: ахборот хавфсизлиги таҳдидларининг халқаро таснифи яратилди (Open Web Application Security Project, АҚШ); биометрик аутентификацияга асосланган амалий дастурларни ишлаб чиқиш усуллари, шунингдек кибер-хавфсизлик когнитив методларидан фойдаланилган (IBM Cyber Security Center of Excellence, АҚШ); Сеул миллий университети олимлари веб-иловаларни шаблон усуллари асосида таҳлил қилиш учун моделлар ишлаб чиқдилар (Seoul National University, Жанубий Корея); амалий дастур таҳлили асосида apache mod_security модули асосида веб-иловаларни ҳимоя қилиш усуллари ишлаб чиқилган (Москва давлат университети, Россия Федерацияси; University of South Wales, Буюк Британия).

Жаҳонда веб-иловалардаги заифликларни аниқлаш учун моделлар ва усулларни ишлаб чиқиш, веб-иловалардаги заифликларнинг халқаро

таснифини ишлаб чиқиш ва янгилаш, веб-иловаларда ишлаётганда аномалияларни аниқлаш учун моделларни яратиш ва веб-иловаларни кириш ва бузиш учун синов усуллари бўйича бир қатор устувор соҳаларда тадқиқотлар олиб борилмоқда.

Муаммонинг ўрганилганлик даражаси. Ахборот хавфсизлиги тизимини ривожлантиришнинг назарий ва амалий масалалари, электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари ва моделлари А.И. Галатенко, В.Н. Опанасенко, В.А. Герасименко, Д. Деннинг, П. Зегжда, А. Грушо, М.Р. Кострова, А.П.Тихонова каби кўплаб хорижий олимларнинг илмий ишларига бағишланган.

Мамлакатимизда ахборотни ҳимоя қилиш, хусусан, электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш муаммолари Т.Ф. Бекмуратов, М.М. Комилов, М.М. Арипов, М.М. Каримов, С.К. Ганиев, Р. Х Ҳамдамов, Б.Ф. Абдурахимов, А.Х. Нишанов, А.В. Кабулов, А.А. Ганиев, О.П. Ахмедова, Р.И.Исаев каби олимларнинг изланишларида ўрганилган.

Ҳозиргача электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун етарли назарий асосга эга моделлар ишлаб чиқилмаган. Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари ва моделларини назарий ва амалий ўрганиш, веб-иловалар хавфсизлигини таъминлаш билан боғлиқ муаммоларни ҳал қилиш етарли даражада тадқиқ қилинмаган.

Диссертация тадқиқотининг диссертация бажарилган илмий тадқиқот муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқотлари Муҳаммад ал-Хоразмий номидаги Тошкент Ахборот Технологиялари Университетида илмий-тадқиқот ишлари режасининг ФА5-005 "Ахборот хавфсизлиги таҳдидларидан давлат Интернет-ресурсларини ҳимоя қилиш усуллари ва дастурларини ишлаб чиқиш" (2015-2016); А5-075 "Электрон тармоқ ресурслари хавфсизлигини таъминлаш учун алгоритмлар ва дастурий таъминотни ишлаб чиқиш" (2015-2017); БВ-Атаб-2018-568 "Электрон ресурсларнинг маълумотларини ҳимоя қилиш тўғрисида қарор қабул қилишни қўллаб-қувватлаш учун ахборот хавфини бошқариш учун ақлли дастурий тизимларни яратиш" (2018-2019); ЁБВ-Атеч-2018-212 "Электрон ҳукумат тизимларида ахборот ресурслари хавфсизлигини таъминлаш усуллари ва алгоритмларини ўрганиш ва ишлаб чиқиш" (2018-2019) лойиҳалари доирасида олиб борилган.

Тадқиқотнинг мақсади электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун имзо ва хулқ-атвор таҳлилига асосланган мослашувчан моделлар ва усулларни ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

электрон ресурсларда ахборот хавфсизлигига таҳдидларнинг характерли маконини шакллантириш;

электрон ресурсларда ахборот хавфсизлигига таҳдид солувчи имзолар базасини яратиш;

параметрик идентификация асосида электрон ресурсларда ахборот хавфсизлигига таҳдидларни таснифлаш алгоритмларини ишлаб чиқиш;

веб-иловалар учун хавфсизлик девори ёрдамида электрон ресурсларни ҳимоя қилиш усулларини ишлаб чиқиш;

электрон ресурсларда ахборот хавфсизлигига таҳдидларни аниқлаш учун параметрик идентификациялашнинг мослашувчан моделларини ишлаб чиқиш;

мустақил ечимлар асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари ва алгоритмларини ишлаб чиқиш;

хулқ-атвор таҳлили асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун мослашувчан моделни ишлаб чиқиш;

электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилувчи дастурий воситани ишлаб чиқиш.

Тадқиқотнинг объекти сифатида электрон ресурслар ва веб-иловалар хавфсизлигини таъминлаш жараёнлари қаралган.

Тадқиқотнинг предмети электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишнинг моделлари, усуллари ва алгоритмлари.

Тадқиқотнинг усуллари. Ишда ахборот хавфсизлиги ва маълумотларни кидириш усуллари қўлланилади: хусусиятларни дастлабки тавсифлаш учун шаблон усули, дастлабки тавсиф майдонида хусусиятларни яратиш алгоритмик усули, веб-иловалар учун хавфсизлик девори ёрдамида SQL инъекцияси ва электрон ресурсларни ҳужумлардан ҳимоя килиш XSS усули, шунингдек алгоритмлар, параметрик идентификациялаш асосида электрон ресурсларда ахборот хавфсизлигига таҳдидларни таснифлаш.

Тадқиқотнинг илмий янгилиги:

объект-хусусиятлар жадвалининг ўзаро таъсирига асосланган ҳолда электрон ресурслардаги ахборот хавфсизлиги таҳдиди сигнатураларининг белгили фазоси ва маълумотлар базаси яратилган;

параметрли идентификация қилиш усуллари асосида электрон ресурсларда ахборот хавфсизлиги таҳдидларини таснифлаш алгоритмлари ишлаб чиқилган;

веб-иловалар брандмауэр технологиясига асосланган электрон ресурсларни SQL (Structured Query Language) инъекцияси ва XSS (Cross-Site Scripting) каби ҳужумлардан ҳимоя қилиш усуллари ишлаб чиқилган;

сигнатура ва хулқ-атвор таҳлили асосида электрон ресурсларни ҳимоя қилиш учун мослашувчан моделлар ишлаб чиқилган;

тилга боғлиқ бўлмаган ечимлар асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя килишнинг усуллари ва алгоритмлари ишлаб чиқилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

электрон ресурсларда ахборот хавфсизлигига таҳдидларни аниқлашга имкон берадиган параметрик идентификациялаш асосида электрон ресурсларда ахборот хавфсизлигига таҳдидларни таснифлаш алгоритмлари ишлаб чиқилган;

электрон ресурсларни ахборот хавфсизлигига маълум ва номаълум таҳдидлардан ҳимоя қилишга имкон берадиган веб-иловалар учун хавфсизлик девори ёрдамида ҳимоя қилиш усуллари ишлаб чиқилган;

Электрон ресурсларни номаълум турдаги ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун параметрик идентификациялашнинг мослаштирилган моделлари ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги параметрик идентификациялашнинг мослашувчан усуллари, математик ҳисоб-китобларнинг қатъийлиги, овозли ечим усулларидан фойдаланиш, веб-иловалар учун хавфсизлик девори технологиясига асосланган ҳисоблаш алгоритмлари ва усулларининг мос келишини ўрганиш, муаммони тўғри шакллантириш билан асосланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти адаптив параметрик идентификация тамойиллари ва усулларига асосланган электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишнинг мослашувчан моделлари ва усулларини ишлаб чиқиш билан изоҳланади. Шунингдек, Тилга боғлиқ бўлмаган эчимлар асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари ва алгоритмлари ишлаб чиқилган.

Тадқиқот натижаларининг амалий аҳамияти таклиф этилаётган моделлар ва усуллар ҳар қандай бошқарув тизимларида яратилган электрон ресурсларни самарали ҳимоя қилиш имконини берадиган тегишли дастурий таъминотни ишлаб чиқиш билан асосланади. Ушбу моделлар ва усуллар электрон ресурсларни номаълум турдаги ахборот хавфсизлиги таҳдидларидан ҳимоя қилишга имкон берди.

Тадқиқот натижаларининг жорий қилиниши. Ахборот хавфсизлиги таҳдидларидан электрон ресурсларни ҳимоя қилишни таъминлаш учун олинган илмий натижалар асосида:

объект-хусусиятлар жадвалининг ўзаро таъсирига асосланган ҳолда электрон ресурслардаги ахборот хавфсизлиги таҳдиди сигнатураларининг белгили фазоси ва маълумотлар базаси ва улар асосида ишлаб чиқилган дастурий восита Ахборот хавфсизлиги ва жамоат тартибини таъминлашга кўмаклашиш марказига жорий қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 30 мартдаги 33-8/1922-сон маълумотномаси). Илмий тадқиқотлар натижаларидан фойдаланиш электрон ресурсларда зарарли мавжудлигига оператив холатни 1,5 бараварга ошириш, шунингдек веб-ресурслар хавфсизлигини 12 фоизга ошириш имконини берган;

SQL инъекцияси ва XSS каби ҳужумлардан электрон ресурсларни ҳимоя қилишни таъминлашнинг веб-иловалар брандмауэр технологиясига асосланган усуллари ва улар асосида ишлаб чиқилган дастурий восита "Ўзбектелеком" АК ТТТ филиалига жорий етилган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 30 мартдаги 33-8/1922-сон

маълумотномаси). Илмий тадқиқотлар натижаларидан фойдаланиш электрон ресурсларда зарфлик мавжудлигига оператив холатни 1,7 баравар оширишга, шунингдек веб-ресурслар хавфсизлигини 18 фоизга оширишга имкон берган;

параметрик идентификациялаш усуллари асосида электрон ресурслардаги ахборот хавфсизлиги таҳдидларини таснифлаш алгоритмлари, шунингдек веб-иловалар брандмауэр технологияси асосида электрон ресурсларни ҳимоя қилиш усуллари ва улар асосида ишлаб чиқилган дастурий восита "Ўзбекистон темир йўллари" АК Ахборот хавфсизлиги ва ахборотни ривожлантириш дирекциясига жорий қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 30 мартдаги 33-8/1922-сон маълумотномаси). Илмий тадқиқотлар натижаларидан фойдаланиш электрон ресурсларда зарфлик мавжудлигига жавоб бериш вақтини 50% га қамайтириш, шунингдек веб-ресурслар хавфсизлигини 50% га ошириш имконини берган;

электрон ресурсларни ахборот хавфсизлиги таҳдидларидан тилга бохлиқмас сечимлар асосида ҳимоя қилиш усуллари ва алгоритмлари ва улар асосида ишлаб чиқилган дастурий восита "SKIF" МЧЖ фаолиятига жорий қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 30 мартдаги 33-8/1922-сон маълумотномаси). Илмий тадқиқотлар натижаларидан фойдаланиш электрон ресурсларда зарфлик мавжудлигига оператив холатни 2 баравар оширишга, шунингдек веб-ресурслар хавфсизлигини 30 фоизга оширишга имкон берган.

объект-хусусиятлар жадвалининг ўзаро таъсирига асосланган холда электрон ресурслардаги ахборот хавфсизлиги таҳдиди сигнатураларининг белгили фазоси ва маълумотлар базаси, ҳамда параметрик идентификациялаш усуллари асосида электрон ресурслардаги ахборот хавфсизлиги таҳдидларини таснифлаш алгоритмлари ва улар асосида ишлаб чиқилган дастурий восита "SMART SOFTWARE" МЧЖ фаолиятига қўлланилган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 30 мартдаги 33-8/1922-сон маълумотномаси). Илмий тадқиқотлар натижаларидан фойдаланиш электрон ресурсларда зарфлик мавжудлигига оператив холатни 2,5 баравар оширишга, шунингдек веб-ресурслар хавфсизлигини 50 фоизга ошириш имконини берган;

SQL инъекцияси ва XSS каби ҳужумлардан электрон ресурсларни ҳимоя қилишни таъминлашнинг веб-иловалар брандмауэр технологиясига асосланган усуллари ҳамда сигнатура ва хулқ-атвор таҳлили асосида электрон ресурсларни ҳимоя қилиш учун мослашувчан моделлар ва улар асосида ишлаб чиқилган дастурий восита ООО "SOFTWARE DESIGN" фаолиятига қўлланилган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 30 мартдаги 33-8/1922-сон маълумотномаси). Илмий тадқиқотлар натижаларидан фойдаланиш электрон ресурсларда зарфлик мавжудлигига

оператив ҳолатни 1,1 баравар ошириш, шунингдек веб-ресурслар хавфсизлигини 25 фоизга ошириш имконини берган.

Тадқиқот натижаларининг апробацияси. Диссертациянинг асосий назарий ва амалий натижалари 3 та халқаро ва 2 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилиниши. Тадқиқотнинг асосий натижалари 29 та илмий ишларда эълон қилинган, улардан 18 таси Ўзбекистон Республикаси Олий аттестация комиссияси томонидан докторлик диссертацияларининг асосий илмий натижаларини эълон қилиш учун тавсия қилинган журналларда, жумладан 3 таси хорижий журналларда ва 15 таси республика журналларида нашр қилинган ҳамда 4 та ЭҲМ учун дастурларни расмий рўйхатдан олинганлиги тўғрисидаги гувоҳнома олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация кириш, бешта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертациянинг ҳажми 194 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Киришда диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республикаси фан ва технологияларини ривожлантиришнинг устувор йўналишларига мувофиқлиги баён қилинган, тадқиқотнинг мақсади ва вазифалари, объекти ва мавзуси ифодаланган, илмий янгилик, амалий тадқиқотлар натижаларини баён қилинган, олинган натижаларнинг ишончлилиги асосланган, олинган натижаларнинг назарий ва амалий аҳамиятини очиб берилган, тадқиқотлар, тадқиқот натижаларини жорий этиш, натижаларнинг нашр этилиши ва диссертациянинг тузилиши тўғрисида маълумотлар берилган.

Диссертациянинг «**Электрон ресурсларни ахборот хавфсизлиги таҳдидлардан ҳимоясини таъминлашнинг мослашувчан моделлари ва усуллари**» деб номланган биринчи бўлимида оммабоп ахборот хавфсизлиги таҳдидларининг ҳозирги ҳолати таҳлил қилинган, ривожланиш тенденциялари ва электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишнинг замонавий усуллари ва моделлари ўрганилган. Мавжуд дастурий воситалар электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун тавсифланган.

Энг кенг тарқалган таҳдидлар қуйидаги гуруҳларга бўлиб, ўрганилган:

- серверда кодни масофадан туриб бажариш;
- SQL - қарши;
- XPath - қарши;
- файлни серверда масофадан туриб ишга тушириш;
- маҳаллий файлни ишга тушириш;
- XSS типидаги ахборот хавфсизлиги таҳдиди;
- CSRF турининг ахборот хавфсизлиги таҳдиди.

Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишнинг мавжуд моделлари кўриб чиқилган, натижада иккита турдаги

моделлар мавжудлиги аниқланди, улар имзо (шаблон) ва фойдаланувчи ва тизимнинг хатти-ҳаракатларини (хулқ-атворини) таҳлил қилиш учун моделлардир. Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишнинг имзо моделларига учта модель киради:

- Андоза излаш модели,
- Ҳозирги ҳолатнинг намунавий таҳлили,
- Биологик моделлар.

Хулқ моделлари ишлашининг алгоритми - бу тизимнинг нормал хатти-ҳаракати ва ҳозирги ҳолат ўртасидаги тафовутларни топиш. Агар номувофиқликлар аниқланса, бундай вазият топилган ИС таҳдид деб ҳисобланади.

Диссертациянинг «**Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишнинг мослаштирилган моделлари ва алгоритмлари**» деб номланган иккинчи бобидада ахборот тизимларини ахборот хавфсизлиги таҳдидларидан мослашувчан ҳимоя қилиш тушунчаси келтирилган. Иккинчи бўлимда, таниб олиш функциясидан фойдаланиб, SQL қарши ҳужумини аниқлаш учун алгоритм ва сунъий маълумотлардан фойдаланган ҳолда тавсия этилган алгоритмнинг самарадорлигини баҳолаш таклиф этилади. Шунингдек, ахборот объекти модели таклиф этилади. Ушбу модель асосида веб-иловаларга XSS ҳужумларини аниқлаш алгоритми пайдо бўлиши частотаси ва кирувчи сўровларни тузишда иштирок этувчи белгиларнинг аҳамияти коэффициенти ҳисобга олинган ҳолда тузилган. Аномалияларни аниқлаш асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун мослашувчан модель ишлаб чиқилган.

2.1-бўлимда электрон ресурсларни ахборот хавфсизлиги таҳдидларидан мослашувчан ҳимоя қилиш тушунчаси таклиф қилинади.

Электрон ресурсларни ўз ичига олган тўртта даража кўриб чиқилади:

1. Веб-илова даражаси, яъни бу даража фойдаланувчилар билан алоқаларни амалга оширади. Масалан, маиший техникаларни сотиш порталининг электрон ресурси, ташкилотларнинг турли веб-сайтлари ва бошқалар.

2. Маълумотлар базалари билан ишлаш даражаси, яъни бу даража тизим маълумотларини қайта ишлайди, шунингдек маълумотларни сақлайди. Масалан: Mysql, Postgresql.

3. ОТ билан ишлаш даражаси, яъни ушбу даража веб-сервер, таржимон, тизимнинг асосий ядроси ва бошқалар каби тизимнинг барча таркибий қисмлари учун жавобгардир.

4. Тармоқ билан ишлаш даражаси, бу даража фойдаланувчилар ва электрон ресурсларнинг тармоқдаги ўзаро таъсири учун жавобгардир.

Электрон ресурснинг мослашувчан хавфсизлиги қуйидаги таркибий қисмларни ўз ичига олади:

- Ахборот хавфсизлигига таҳдидларни таснифлаш алгоритмлари;
- Электрон ресурсларни ахборот хавфсизлиги таҳдидидан ҳимоя қилишнинг мослашувчан моделлари,

- Электрон ресурсларни оммабоп ИС таҳдидларидан ҳимоя қилишнинг адаптив усуллари.

1-расм. Электрон ресурснинг барча инфратузилма элементлари билан ўзаро таъсири схемаси

Юқоридаги ҳар қандай элементга ҳужум қилиниши мумкин, натижада электрон ресурс таъсир қилади. Мослашув механизми сизга яхши маълум бўлган ва бошқариладиган воситалардан фойдаланган ҳолда, ахборот хавфсизлиги таҳдидларини аниқлаш ва қарор қабул қилиш имконини беради.

Адаптив хавфсизлик элементи электрон ресурсни ҳимоя қилишни таҳлил қилиш, янги ахборот хавфсизлиги таҳдидлари тўғрисида маълумотларни узатиш ва янгилаш функцияларини ўзгартириш учун жавобгардир. Масалан, ахборот хавфсизлиги таҳдидларини аниқлашга имкон берадиган имзоларни янгилаш. Адаптив элемент маълум ҳаракатлар тўғрисида билдиришнома ҳам бериши мумкин, хусусан:

- sms, телеграм ёки электрон почта шаклида хабарномани амалга ошириш;
- ҳужумларни аниқлаш ва уларни дарҳол блокировка қилиш;
- маълум бир ахборот хавфсизлиги таҳдидини бартараф этиш бўйича тавсиялар ишлаб чиқиш.

2.2.1- бўлимда имзоларни таҳлил қилиш асосида ахборот хавфсизлигига таҳдидларни таснифлаш алгоритмлари кўрсатилган. Электрон ресурсларда ахборот хавфсизлигига таҳдидларни таснифлаш учун кириш сатрига боғлиқ бўлган пастдан чекланган функциядан фойдаланган ҳолда ҳужумларни аниқлашнинг математик усули ишлаб чиқилган. Бундай функцияни қуриш учун зарарли ҳужумларни ташкил этишда кўпинча фойдаланиладиган махсус белгилар ва калит сўзлар ишлатилган. SQL, XSS инъекцияси электрон ресурсларда оммабоп ахборот хавфсизлиги таҳдидларига асосланган таснифлаш алгоритмининг ишлашини кўриб чиқамиз.

SQL инъекцияси ахборот хавфсизлигига таҳдиди веб-саҳифадаги форма орқали киритилган имзо ёрдамида ёки кириш параметрларини ўзгартиришга имкон берадиган бошқа усул билан амалга оширилади. Келинг, SQL инъекциясининг мисолини кўриб чиқайлик. Сўровлар form.php манзилига юборилади. Ушбу файлда қуйидагилар ёзилади:ққк

$test = $_GET['test'];

$query = "SELECT * FROM userlist WHERE user='$test";

Бу ерда маълумотлар $test ўзгарувчисининг қиймати бўйича намуна олинади. Кейин тирноқ белгиси билан сўров юборилади:

site.uz/index2.php?user=KamilPHP'

Агар ушбу сўров бажарилгандан кейин хато юз берса, унда SQL инъекциясининг заифлиги юзага келади. Кейинчалик, ушбу белгилар гуруҳини ишлатиб, кириш сатри ҳужумлиги ёки ҳужум эмаслиги аниқланади. Бунинг учун махсус белгилар асосида кирувчи сатр оддий талаб ёки ҳужум эканлигини аниқлайдиган алгоритмни ишлаб чиқиш керак.

1-жадвал

Объект атрибути (махсус белгилар)

Ўзгарувчан	Белги
u_1	Бўшлиқ
u_2	Нуқтали вергул (;)
u_3	Апостроф (')
u_4	Ўнг қавс ())
u_5	Чап қавс (()
u_6	Ўнг жингалак қавс (})
u_7	Чап жингалак қавс ({)
u_8	Тўғри квадрат қавс (])
u_9	Чап квадрат қавс ([)
u_{10}	Кескин (#)
u_{11}	Фоиз (%)
u_{12}	Қўштирноқ (")
u_{13}	Амперсанд (&)
u_{14}	Орқа чизиқ (\)
u_{15}	Вертикал чизиқ (|)
u_{16}	Тенглик белгиси (=)
u_{17}	(>) дан катта
u_{18}	Қамроқ (<)
u_{19}	Юлдузча (*)
u_{20}	Слеш (/)

2-жадвал

Объект ёрлиғи (махсус калит сўзлар)

Ўзгарувчан	Калит сўзлар
u_{21}	and
u_{22}	or
u_{23}	union
u_{24}	where
u_{25}	limit
u_{26}	group by
u_{27}	select
u_{28}	\'
u_{29}	hex
u_{30}	substr

SQL инъекциясини аниқлаш учун 1-жадвалнинг махсус белгиларидан ва 2-жадвалнинг махсус калит сўзлардан фойдаланган ҳолда SQL ҳужумларининг хусусиятлари ўрганилади. Ихтиёрий L кириш сўровини кузатадиган бўлсак, бунда ушбу сўровдаги $x_1, x_2, \dots, x_{20}$лар 1-жадвалидаги махсус белгилар частоталарини, ва $x_{21}, x_{22}, \dots x_{30}$лар 2-жадвалдаги калит сўзлар частоталарини, x_{31}– бу L сўровдаги 0,1,2, ..., 9 рақамлар ва барча ҳарфларнинг пайдо бўлиш частотасини ифодалайди. SQL инъекция ҳужумларини аниқлаш нуқтаи назаридан a, b, ... z ҳарфлари ва 0, 1, ..., 9 рақамлари муҳим рол ўйнамайди. Шунинг учун, биз кузатаётган L сўровдаги барча ҳарфлар ва рақамларнинг пайдо бўлиш частотаси 1 га тенг деб ҳисоблаймиз.

Шунда x_{31}=1 бўлади. Шундай қилиб, ҳар қандай L сўровни қуйидаги хусусиятлар ёрдамида аниқлаш мумкин: L=$x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}$, яъни X фазонинг элементларни сифатида. SQL инъекция ҳужумларини киришда кўпинча қуйидаги жадвалларда кўрсатилган махсус белгилар ва махсус калит сўзлардан фойдаланилади.

Аниқлаш алгоритми. L таърифи шуни кўрсатадики, X тўпламда яратилган ҳар қандай L элемент $\Gamma = \{L = (x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}) : x_{31} = 1\}$ гипертекисликда ётади. Ушбу гипертекислик тенгламасидан фойдаланиб, кириш сатрида махсус белгилар ва калит сўзларнинг пайдо бўлиш частотаси канчалик юкори бўлса, L кириш сатрининг SQL инъекция ҳужумларига яқинлиги шунчалик равшан бўлишини тахмин қилиш мумкин. Шунинг учун ҳужумни аниқлаш функцияси $x_1, x_2, \dots, x_{20}, x_2, \dots x_{30}$ ўзгарувчиларига нисбатан ортиши ва x_{31} ўзгарувчига нисбатан камайиши керак. Шунга асосланиб, SQL инъекция ҳужумларини аниқлаш учун $x_1, x_2, \dots, x_{20}, x_{21}, \dots x_{30}$ да ўсадиган қуйидаги функцияни таклиф қиламиз:

$$f(L) = f(x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}) = \frac{\sum_{i=1}^{30} x_i}{\sum_{i=1}^{30} x_i + x_{31}}$$

Сатрда барча бошқа ҳарфлар ва 0,1, 2, ... 9 рақамларининг пайдо бўлиш частотаси 1 га тенг, Шунда охирги ифодадан қуйидагини ҳосил қиламиз:

$$f(L) = f(x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}) = \frac{\sum_{i=1}^{30} x_i}{\sum_{i=1}^{30} x_i + 1} \quad (1)$$

Ушбу функция қуйидаги хусусиятларга эга:

1) $0 \le f(L) < 1$ барча $L \in \Gamma$ учун.

2) SQL инъекция ҳужумлари учун пастдан функциянинг минимал қиймати 1/2 билан чекланган.

Шундай қилиб, агар кириш сўрови SQL инъекция ҳужуми бўлса, унда ушбу сўров ҳеч бўлмаганда биринчи жадвалдаги битта махсус белгини ёки иккинчи жадвалдаги битта калит сўзни ўз ичига олиши керак. Шунинг учун $\sum_{i=1}^{30} x_i \ge 1$ ва $f(L)$ функцияси x_i ўзгарувчининг ҳар бирида кўпаяётганлиги сабабли, унинг минимуми $\sum_{i=1}^{30} x_i \ge 1$· L_0 нуқтада эришади ва $\sum_{i=1}^{30} x_i = 1$ бўлади. Шундай қилиб, L ихтиёрий сўров бўлиб, агар SQL инъекция ҳужумларини киришда 2-жадвалдан махсус калит сўзлар ишлатилса, $f(L) \ge$

1/2 бўлса, *L* SQL инъекция ҳужуми бўлиши мумкин; ёки $f(L) < 1/2$ бўлса, унда кириш сўрови нормал ҳисобланади. Шунинг учун (1) функциясини нормал сўровни ва махсус белгилар ва калит сўзлар орқали қурилган SQL инъекция ҳужумларни аниқлашда ишлатса бўлади. Шундай қилиб, агар *L* 1-жадвалдан камида 2 та махсус белгиларни ўз ичига олган ихтиёрий сатр бўлса, у ҳолда $f(L) \geq 2/3$ бўлади ва L эҳтимол SQL инъекция хужумидир, ёки $f(L) < 2/3$ бўлса, кириш сатри нормал бўлиши мумкин. Шунинг учун (1) функцияни нормал сатрларни ва 1-жадвалнинг махсус белгилари ва 2-жадвалнинг махсус калит сўзлари ёрдамида қурилган SQL инъекция ҳужумларни аниқлаш учун ишлатиш мумкин. Иккала ҳолатда ҳам (1) функциядан фойдаланиб, биз таҳдидларни аниқлаш учун сифат мезонига эгамиз. Бизнинг ҳолатда (1) функциясининг аниқланиш чегараси 1/2 рационал сон бўлади. Шундай қилиб, агар *L* сатрида камида битта махсус белги ёки битта калит сўз бўлса, таҳдидни аниқлаш учун $f(L) \geq 1/2$ шарт кифоя қилади.

3-жадвал

SQL инъекциясининг таркибий қисмларига намуна

Номер	Ҳужум каторлари
1	id=1'
2	KamilPHP'
3	KamilPHP'%20--%20test
4	1 UNION SELECT 1,2

4-жадвал

Нормал каторлар намуналари

Номер	Нормал каторлар
1	Test
2	password
3	kamil@
4	@kamil
5	{(1%2)+(3/4)}/5}
6	&temptest(URL){ width,height }

Калит сўзларнинг аҳамиятини ҳисоблаш. 1-жадвалдаги махсус белгиларнинг аҳамиятини аниқлаш учун 39 SQL инъекция ҳужумлари асосида тажриба ҳисоб-китоблар ўтказилди. Бунда қуйидаги формуладан фойдаланилди:

$K_B = \frac{K_U}{K_N}$, бу ерда K_B – U махсус белгисининг аҳамиятлилик даражаси, бундан кейин U белгисининг аҳамиятлилик коэффициенти дейилади, K_U- u махсус белгиси ёрдамида қурилган L SQL инъекция ҳужумлар сони, K_N – SQL инъекция ҳужумларининг умумий сони.

Кейин, киритилган белгиларни ишлатиб, кириш сатрини сонли координаталари бўлган вектор сифатида аниқлаймиз:

$$L = (K_U, x_1, K_U, x_2, \dots, K_{U_{30}} x_{30}, K_{U_{31}} x_{31}) \quad (2)$$

Кириш сатрининг ушбу таърифи аввалгисидан фарқ қилади, чунки кириш сатрининг координаталари (2) бошқасидан фарқ қилади. Шунинг учун, турли хил кириш чизиқлари турли хил координаталарга эга. Аммо, агар X узунлик тушунчасида фойдаланилса, унда баъзи кириш чизиқлари бир хил узунликка эга бўлиши мумкин. Ушбу факт кириш сатрларини фарқлашингизга тўсқинлик қилмайди. (2) га мувофиқ белгиланган кириш-SQL қарши ҳужумининг ўзига хос хусусияти шундан иборатки, у фақат манфий бўлмаган координаталарга эга ва шунинг учун агар сатр узунлиги аниқ ижобий бўлса, унда бу сатр SQL қарши ҳужумига яқин бўлиши мумкин. Шундай қилиб, кириш сатри учун (2) ифода ёрдамида янги аниқлаш функциясини қуриш мумкин. Кейин таниб олиш функцияси кириш сатрини (1) га қараганда аниқроқ аниқлайди, чунки бу ҳолда таниб олиш функциясини тузишда 1, 2 жадвалдаги барча белгиларнинг аҳамиятлилик коэффициенти ҳисобга олинади.

5-жадвал

Махсус Y белгилар учун аҳамиятлилик даражасини аниқлаш

	Махсус Y белгилар учун аҳамияти
=	0.4872
%	0.2051
'	0.6923
*	0.0769
/	0.0513
]	0.0256
[	0.0257
{	0
}	0
&	0
\	0
#	0.0513
"	0
!	0
<	0.0256
>	0.0255
(	0.1538
)	0.1795
;	0
бўшлик	0.7949

Аммо шу билан бирга шуни таъкидлаш керакки, ҳар бир белги аҳамиятлилик коэффициентини аниқлаш учун кўп миқдордаги SQL инъекция ҳужумлари (масалан, 500-600 SQL инъекция ҳужумлари) бўйича тажриба

ҳисоб-китобларни амалга ошириш керак. Ва кейин ҳар бир белгининг аҳамият коэффициентлари деярли барча SQL қарши ҳужумларида бир хил бўлади. Ушбу ҳақиқатни ҳисобга олиб, SQL қарши ҳужумларини аниқлаш учун қуйидаги янги функция таклиф этилади:

$$f_K(L) = f(x_1, x_2, \dots, x_{20}, x_{21}, \dots, x_{31}) = \frac{\sum_{i=1}^{30} K_U x_i}{\sum_{i=1}^{30} K_U x_i + 1} \qquad (3)$$

Энди, (1) функция ўрнига, кириш сатрининг ҳолатини аниқлаш учун (3) функциядан фойдаланиш мумкин. Бу эрда, юқорида айтилганидек, SQL қарши ҳужумларини аниқлаш учун (3) функциянинг пастки чегарасини белгилаш мумкин.

Таниб олиш алгоритми қуйидаги босқичлардан иборат:

1-қадам. Ҳақиқий кириш сатридан фойдаланиб, I. объект (2) га мувофиқ ҳисобланади.

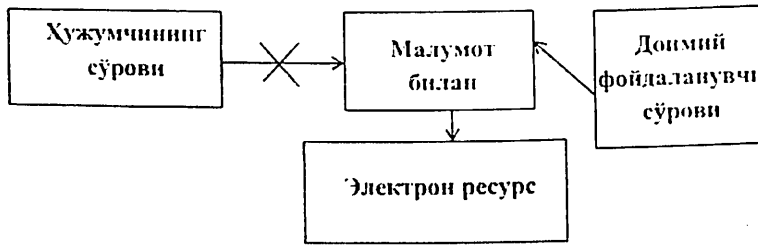
2-қадам. (3) функция қиймати ҳисобланади.

3-қадам. (3) функциянинг минимал қиймати аниқланади (3).

4 босқичли. (3) функция қийматини минимал қиймати билан таққослашда кириш сатрининг ҳолати аниқланади.

Кириш линияларининг ҳолатини аниқлаш учун барча функциялар ахборот объектини моделлаштиришга (кириш чизиқлари) боғлиқлигини кўриш мумкин. Шунинг учун жуда муҳим вазифа кириш сатрини аниқлашни расмийлаштириш тамойилидир. Ушбу муаммонинг ечими асосан ахборот объектларини таниб олишни ҳал қилиш усулларини аниқлайди. Ушбу алгоритм асосида XSS типидаги ахборот хавфсизлигига таҳдид аниқланади.

2.2.1-бўлимида ҳулқ-атвор таҳлили асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун мослашувчан модель ишлаб чиқилган.



2-расм. Адаптив моделнинг схемаси

Ахборот хавфсизлигига таҳдид мавжудлигини кўрсатиши мумкин бўлган HTTP / HTTPS сўровлари қуйидаги алгоритм асосида аниқланади.

1. URL параметрида зарарли белгилар мавжуд бўлган сўровлар;

2. Мавжуд бўлмаган электрон ресурс саҳифаларини сўрашни талаб қилади;

3. Фойдаланувчи-Агент параметри этишмаётган ёки нотўғри тузилган сўровлар;

4. Реферер параметри ўзгартирилган ёки зарарли код мавжуд бўлган сўровлар;

5. Cookie параметри нотўғри ёки зарарли кодни ўз ичига олган сўровлар;

6. Параметрлар узунлиги белгиланган чегаралардан ошиб кетадиган сўровлар.

Қуйида адаптив моделнинг схемаси келтирилган:

1 сўров мисолидан (URL параметрида зарарли белгиларни ўз ичига олган сўровлар) фойдаланиб, ишлаб чиқилган мезонлар кўрсатилади

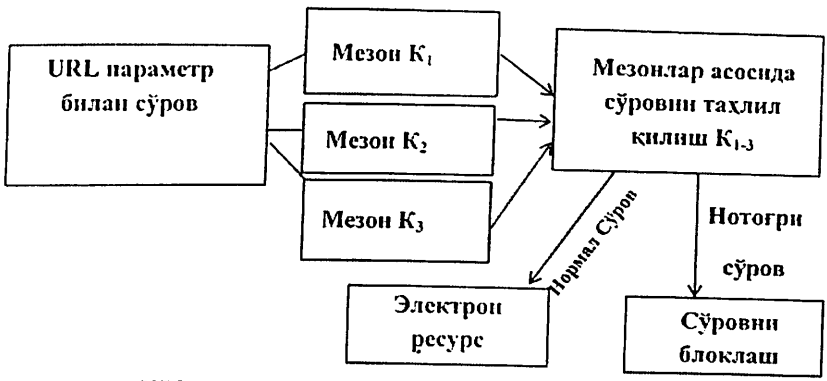
URL манзил учун ишлаб чиқилган мезонлар (3-расм):

К1 - маълум бир электрон ресурс учун созланган URL узунлиги;

К2 - ахборот хавфсизлигига таҳдид мавжудлигини кўрсатувчи баъзи бир махсус белгилар йўқлиги;

К3 - Ахборот хавфсизлигига таҳдид мавжудлигини кўрсатувчи махсус сўзларнинг йўқлиги. Ушбу параметрлар созланиши ва ҳар бир электрон ресурс учун мослаштирилиши мумкин. Ҳар бир зарарли сўров учун ушбу турдаги сўровни аниқлаш мезонлари ишлаб чиқилган. Белгиларнинг умумий сони - 17. Агар электрон ресурсга сўров $\in K_m$, бу эрда mнинг қиймати 1 дан 17 гача бўлса, унда бу сўров электрон ресурсга юборилади, акс ҳолда у блокланади.

Диссертациянинг **"Тилга боғлиқ бўлмаган сўзлар асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари ва алгоритмлари"** деб номланган учинчи боби хизматга йўналтирилган архитектура асосида XSS-ни блокировка қилиш усулларига бағишланган, шунингдек, компьютер тармоғининг электрон ресурсларига рухсатсиз кириш ҳолатларида ахборот хавфсизлиги хавфини баҳолаш тамойилларини тавсифлайди. Компьютер тармоғининг ахборот хавфсизлиги хавфларини баҳолаш муаммоларини ҳал қилиш учун маълумотлар базасининг таркиби кўрсатилган. URL параметрини таҳлил қилиш ва идентификациялаш асосида электрон ресурсни аниқлаш ва ҳимоя қилиш схемаси ишлаб чиқилган (3-расм):



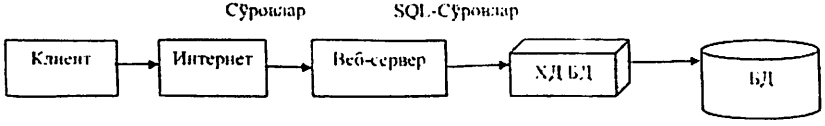
3 - расм. URL параметрини таҳлил қилиш ва идентификациялашга асосланган электрон ресурсни аниқлаш ва ҳимоя қилиш схемаси

3.1-бўлим электрон ресурсларни XSS типидаги ахборот хавфсизлиги таҳдидларидан XML ва XSD ёрдамида ҳимоя қилиш қобилиятига асосланган XSS туридаги ахборот хавфсизлиги таҳдидларини блокировка қилиш усулини ишлаб чиқишга бағишланган. Бу фойдаланувчи томонидан берилган барча шаклларни бошқариш асосида XML ҳужжатини яратишни ўз ичига олади. Ушбу XML ҳужжати серверинг схемаси бўйича текширилади. Ҳар қандай зарарли скрипт яроқсиз ёки нотўғри форматланган XML файлини яратади ва шу билан фойдаланувчига зарарли скриптларни юборишининг олдини олади.

3.2- бўлимда Веб Аппликатион Фиревалл-дан фойдаланиб маълумотлар базасини ҳимоялаш усули кўрсатилган. Усулнинг механизми прокси-серверинг ишлашига асосланган, яъни мижоздан олинган SQL сўровлари аввал маълумотлар базаси серверига эмас, балки ишлаб чиқилган хавфсизлик деворига юборилади. Хавфсизлик девори (ХД) сўровни таҳлил қилади: шубхали деб ҳисобланган сўровлар хавфсизлик девори томонидан блокланади ва бўш натижа мижозга қайтарилади. Акс ҳолда, у сўровни бажариш учун маълумотлар базаси серверини чақиради.

3.4-бўлим заифлик кўрсаткичларини таҳлил қилиш ва ахборот тизимининг элементларини ҳимоя қилиш натижалари асосида компьютер тармоғининг ахборот хавфсизлиги хавфини баҳолаш усулига бағишланган.

Ахборотни ҳимоя қилиш белгиларининг макони шакллантирилди ва компьютер тармоғининг электрон ресурсларига рухсатсиз кириш таҳдидларининг мумкин бўлган вариантлари таҳлили берилган. Ахборот хавфсизлиги хавфларини камайтиришга қаратилган ечимлар келтирилган.

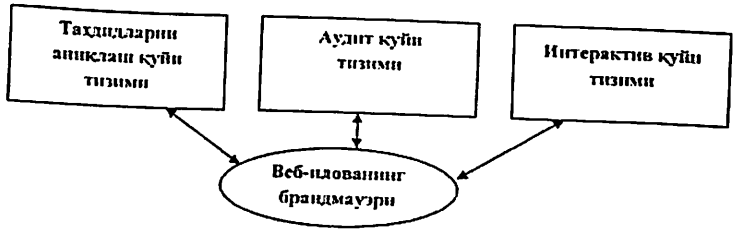


4 - расм. Маълумотлар базаси хавфсизлик девори архитектураси

Диссертациянинг **"Веб-дастурлар девори асосидаги электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усуллари"** деб номланган тўртинчи бўлимни XML асосидаги хавфсизлик девори ёрдамида электрон ресурсларни ҳимоя қилиш усулларига бағишланган. Шунингдек, хавфсизлик девори архитектураси ва фильтрлаш сиёсатининг дизайн масалалари муҳокама қилинади. Уч босқичда фильтрлаш сиёсати: яъни хабарларнинг ҳажмини фильтрлаш, таҳлил қилиш ва XML схемасини текшириш SOAP-нинг яроқли ва яроқсиз хабарлари билан синовдан ўтказилиши муваффақиятли якунлаш асосида қарор кабул қилинади.

4.1-бўлимда веб-иловаларнинг хавфсизлик девори қурилиши тушунчаси кўрсатилган. Веб-иловаларни хавфсизлик девори яратиш учун SQL инъекцияси, сайтлараро скрипт (XSS) ва хизматдан бош тортиш (DOS) каби оммабоп ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш чоралари ишлаб

чиқилган. Веб-иловалар хавфсизлик девори учта қуйи тизимлардан иборат тузилган.

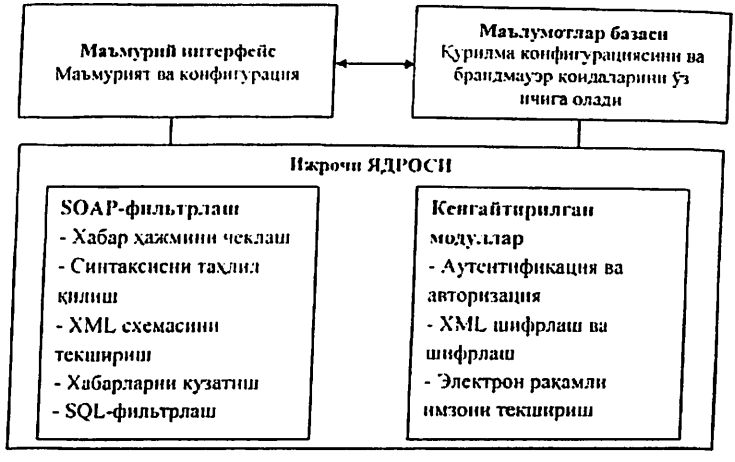


5 – расм. Веб-иловалар брандмауэрининг тузулиши

4.2-бўлимда XML-га асосланган хавфсизлик девори ёрдамида электрон ресурсларни таъминлаш усули муҳокама қилинади.

Фильтрлаш снёсати веб-хизматларга турли хил ҳужумларнинг олдини олиш учун ишлаб чиқилган, масалан:

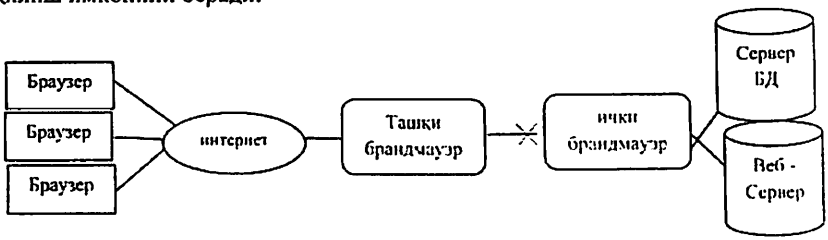
- хабар ҳажмини чеклаш,
- таҳлил қилиш,
- XML схемасини текшириш,
- хабарларни кузатиш,
- SQL-фильтрлаш учун.



6 – расм. XML хавфсизлик девори архитектураси

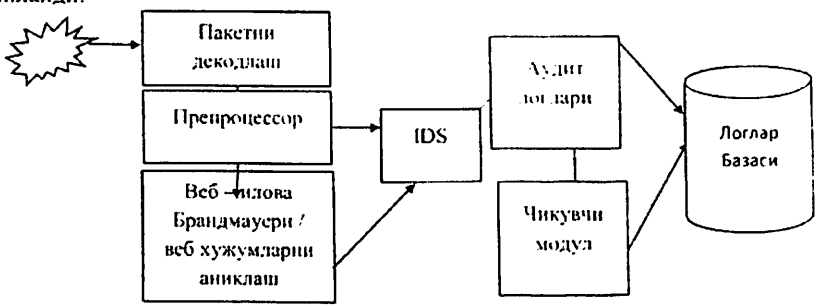
4.3- бўлимда веб-ҳимоя девори ёрдамида электрон ресурсларни ҳимоя қилиш усули баён қилинган. Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун веб-иловаларнинг хавфсизлик девори

механизмидан фойдаланадиган усул ишлаб чиқилган бўлиб, у электрон ресурсларга ҳужум қилишдан олдин ҳужумларни аниқлаш ва олдини олишда юқори даражадаги хавфсизликни таъминлайди. Бу электрон ресурсларга ҳужумларнинг барча турларидан ҳимоя қилади, HTTP трафикни кузатиб бориш ва он-лайн режимида кичик ўзгаришларни ёки доимий ҳолатни таҳлил қилиш имконини беради.



7-расм. Электрон ресурслар учун хавфсизлик девори ташкилий схемаси

Электрон ресурс хавфсизлик девори веб-сервер матосининг бир қисми ёки тармоқдаги тескари прокси сифатида жойлаштирилган. 7-расмда электрон ресурслар учун хавфсизлик деворини ташкил қилиш диаграммаси кўрсатилган. Ҳимояни таъминлаш учун қоидалар ишлаб чиқилиши керак. Қоидаларнинг тўпламидан фойдаланишнинг афзаллиги шундаки, улар имзоларни талаб қилмайди ва кўпинча электрон ресурсларда жойлашган, номаълум турдаги ахборот хавфсизлиги таҳдидларидан ҳимояни таъминлайди.



8-расм. Ишлаб чиқлиган тизимининг архитектураси

Ушбу қоидаларни кўриб чиқиш тавсия этилади:

- HTTP ҳимояси – HTTP протоколининг бузилишини аниқлаш ва маҳаллий фойдаланиш қоидаларини аниқлаш;
- кенг тарқалган веб-хужумлардан ҳимоя қилиш - веб-илова хавфсизлигига типик ҳужумларни аниқлаш;
- автоматлаштиришдан ҳимоя қилиш - ботларни, куртларни, браузерларни ва бошқа зарарли ҳаракатларни аниқлаш;
- троян ҳимояси - троян отларига киришни аниқлаш;

- хатоларни яшириш - серверга юборилган хато хабарларининг бузилиши.

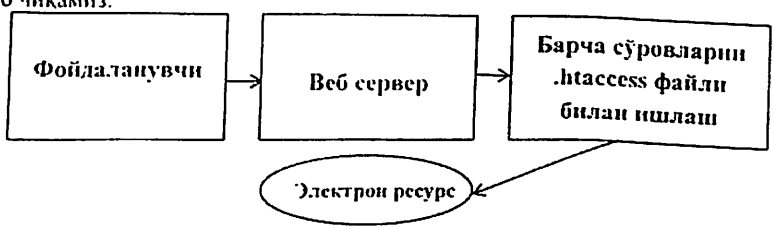
Электрон ресурсларнинг ҳимоясини таъминлаш учун электрон ресурсларнинг хавфсизлигини таъминлаш учун мураккаб архитектура ишлаб чиқилган.

Ахборот хавфсизлигига таҳдидларни олдини олиш учун иккита механизм ишлаб чиқилган:

- .htaccess файлига асосланган;
- index файлига ахборот хавфсизлиги таҳдидини ҳимоя қилиш модулининг уланиш кодини киритиш асосида.

Ҳар бир механизмни батафсил кўриб чиқайлик:

.htaccess файлга асосланган .htaccess файли веб-серверни электрон ресурс ишлаб чиқарувчиси томонидан созлаш учун талаб қилинади. Ушбу файлнинг конфигурациясини ўзгартириш натижасида фойдаланувчи электрон ресурснинг ишлашини ўзгартириши мумкин. Ушбу файл электрон ресурснинг тубида жойлашган ва унинг ишлаш радиуси барча электрон ресурсларга, шу жумладан барча каталог ва пастки каталогларга таъсир қилади. Электрон ресурсга кирадиган барча сўровлар аввал .htaccess файлига ишлов бериш учун ўтади ва шундан кейингина сўровлар ўтади ёки блокланади. htaccess веб-иловасининг хавфсизлик девори қандай ишлашини кўриб чиқамиз.



9-расм. Веб иловалар брандмауэри .htaccess асосида ишлаш схемаси

.htaccess файли электрон ресурс ҳимоя қилинадиган қуйидаги мезон турларини белгилайди:

- асосий саҳифа 404 ва 403 хатоларига ўрнатилди;
- PHP тилининг хавфли функциялари ўчирилган;
- POST ва GETдан ташқари ҳар қандай сўровлар тақиқланади;
- электрон ресурсдан конфигурация ва паролларга эга файлларга кириш блокланган;
- паролларни ўз ичига олган тизим файлларига кириш тақиқланади;
- сайтга қора рўйхатдаги кириш тўсиб қўйилган;
- нотўғри UserAgent билан сайтга кириш блокланган;
- SQL инъекциясидан ва сайтлараро скриптлардан ҳимоя қилиш;
- тизим каталогларига кириш блокланган.

Бу ерда SQL инъекциясини ҳимоя қилиш қандай ишлаши кўриб чиқилади:

RewriteEngine On
RewriteCond %{THE_REQUEST} union[^\(]\(*
RewriteCond%{THE_REQUEST}(;|<|>|'|"|\).(*|union|select|insert|drop|delete|update|create|alter|script|encode)*

Ахборот хавфсизлиги таҳдидидан ҳимоя қилиш модулининг уланиш кодини индекс файлига киритиш асосида Электрон ресурс кўплаб веб-серверлар билан ишлаши мумкин, аммо .htaccess файли фақат apache веб-серверида (энг машҳур веб-сервер) мавжуд. Бошқа веб-серверларни қамраб олиш учун ахборот хавфсизлиги таҳдидини ҳимоя қилиш модулининг уланиш кодини индекс файлига киритиш учун асосий механизм ишлаб чиқилган.Ушбу механизм кутубхонани барча сўровларни таҳлил қиладиган индекс файлига улашга асосланган. Ушбу механизм махсус техник ресурсларсиз электрон ресурсни ахборот ҳимояси таҳдидларидан ҳимоя қилишга имкон беради, шунингдек, SSL ишлатилаётган жойда сўровларни таҳлил қилиш имконияти мавжуд, чунки ҳимоя электрон ресурснинг ўзи веб-серверида жойлашган.

Диссертациянинг **"Электрон ресурсларни ахборот хавфсизлиги таҳдидлардан ҳимоясини таъминлашнинг мослашувчан моделлари ва усуллари"** деб номланган бешинчи бобида мослашувчан моделлар ва усуллар асосида ишлаб чиқилган "Adaptive Web protector" дастурий таъминоти электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишга имкон беради.

ХУЛОСА

«Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоясини таъминлашнинг мослашувчан моделлари ва усуллари» мавзуси бўйича олиб борилган тадқиқот натижалари асосида қуйидаги асосий хулосалар тақдим этилди:

1. Электрон ресурсларни ахборот ҳимояси таҳдидларидан ҳимоя қилишнинг мослашувчан моделлари ва усулларини ишлаб чиқиш мақсадга мувофиқлиги ва истиқболлари асосланди. Диссертация ишида қўйилган мақсад ва вазифалар тўлиқ бажарилган.

2. Электрон ресурсларни ахборот хавфсизлиги таҳдидларидан адаптив ҳимоя қилиш концепцияси таклиф этилади, бу эса имзо ва хатти-харакатлар таҳлилидан фойдаланган ҳолда ресурсларни адаптив ҳимоя қилиш чораларини ишлаб чиқиш имконини беради.

3. SQL инъекция ҳужумларини аниқлаш функцияси ёрдамида аниқлаш ва сунъий маълумотлардан фойдаланган ҳолда тавсия этилган алгоритмнинг самарадорлигини баҳолаш алгоритми яратилди. Таклиф қилинаётган алгоритм ҳужум ва одатий аниқланишлар билан, шунингдек, ҳужум ва оддий сатрларнинг тахминий маълумотларини ишлатиб, олдиндан маълум бўлган чегаралар билан бирлаштирилган белгилар тўпламини яратади. Ушбу алгоритм имзо таҳлили асосида SQL инъекцияси каби ахборот хавфсизлиги таҳдидларини аниқлашга имкон беради. SQL инъекцияси ва XSS каби

электрон ресурсларни ахборот химояси таҳдидларидан ҳимоялашни таъминлаш усулларининг жорий этилиши қуйидагиларга имкон берди: электрон ресурсларда заифликлар мавжудлигига оператив холатни 1,7 баравар ошириш, веб-ресурсларнинг хавфсизлигини 18 %га ошириш, шунингдек, ахборот хавфсизлиги ва бардошлилигини таъминлаш харажатларини 20%га камайтириш имконини берди.

4. Хулқ-атвор таҳлили асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш учун мослашувчан модель ишлаб чиқилган, бу модель электрон ресурсларни ҳам маълумотлар базасида мавжуд бўлган таҳдидлардан ҳам ахборот хавфсизсиги таҳдидларидан ҳимоя қилишга имкон беради. Ахборот хавфсизлиги таҳдидларининг яратилган характерли маконини, электрон ресурсларда ахборот хавфсизлиги таҳдидларини таснифлаш алгоритмларини жорий этиш, электрон ресурсларда заифликлар мавжудлигига оператив холатни 2,5 баравар оширишга, веб-ресурсларнинг хавфсизлигини 50 %га оширишга, шунингдек, ахборот хавфсизлиги ва носозликларга чидамлилигини таъминлаш харажатларини 30%га камайтиришга имкон берди.

5. Электрон ресурсларни ҳимоя қилиш учун мавжуд моделларнинг киёсий таҳлили ва электрон ресурсларни ҳимоя қилишнинг адаптив модели билан киёсий таҳлил натижаларига кўра, адаптив модель тўпланган баллар сони жиҳатидан афзалликларга эга эканлиги аниқланди (9).

6. Сервисга асосланган архитектурага асосланган XSS-ни блокировка қилиш усули ишлаб чиқилган бўлиб, бу энг машҳур дастурлаш тилларида ёзилган электрон ресурсларни ҳимоя қилиш имконини беради.

7. Ахборот хавфсизлиги хавфини баҳолаш тамойиллари компьютер тармоғининг электрон ресурсларига рухсатсиз кириш учун компьютер тармоғининг электрон ресурсларига рухсатсиз кириш хавфи белгиларини тан олишга асосланган ҳолда ишлаб чиқилган, бу ўз навбатида электрон ресурс учун юзага келиши мумкин бўлган хатарларни аниқлашга имкон беради.

8. Веб-иловаларнинг маълумотлар базаларини ахборот хавфсизлиги таҳдидларидан ҳимоя қилиш усули ишлаб чиқилган, маълумотлар базалари учун хавфсизлик девори ишини баҳолаш амалга оширилган.

Ушбу усул хавфсизлик девори асосида маълумотлар базаси ҳимоясини яратишга имкон беради, бу SQL инъекцияси каби ахборот хавфсизлиги таҳдидларидан маълумотларни ҳимоя қилади. Электрон ресурсларнинг хавфсизлиги 30% дан 100% гача ошади, бу электрон ресурс қайси платформада яратилганига боғлиқ. Drupal, Wordpress, Joomla каби машҳур веб-сайтларни бошқариш тизимларининг ҳимоясини таъминлаш, шунингдек веб-сайтга сўровларни фильтрлаш механизми жорий этилиши: электрон ресурслардаги заифликларга оператив холатни 2 баравар ошириш, веб-ресурсларнинг хавфсизлигини 30 %га ошириш, харажатларни камайтириш. ахборот хавфсизлиги ва барқарорлигини 30% га ошириш имкониятини яратади.

9. Электрон ресурс саҳифаларида вирусларни аниқлаш усули ишлаб чиқилган, бу электрон ресурсни зарарли таркибдан ҳимоя қилишга имкон

беради. Ушбу усул веб-дастурлар орасида таркаладиган аник веб-вирусларни аниклаш имконини беради.

10. Веб-дастурлар девори қурилиши концепцияси таклиф этилади. Бу веб-илова девори асосида электрон ресурсларни ҳимоя қилиш усулларини ишлаб чиқиш бўйича чора-тадбирларни аниклашга имкон беради.

11. XML технологиясидан фойдаланган холда веб-дастурлар девори асосидаги электрон ресурсларни ҳимоя қилиш усули ишлаб чиқилган ва хавфсизлик девори архитектурасини лойиҳалаш ва фильтрлаш сиёсати кўриб чикилган. Уч фильтрлаш сиёсати, яъни хабарлар ҳажмини фильтрлаш, таҳлил қилиш ва XML схемасини текшириш муваффақиятли бажарилди. Улар яроқли ва яроқсиз SOAP хабарлари билан синовдан ўтган. Ушбу усул фойдаланувчига SOAP хабарларидаги ҳужум элементларини аниқлаш ва хабарларни блокировка қилишга имкон беради. Шундай қилиб, веб-хизматларга турли хил ҳужумларнинг олдини олиш мумкин. Ушбу усулнинг қўлланилиши барча кирувчи трафик фильтрланганлиги ва ушбу усул электрон ресурс ишлаб чиқилаётган тилга боғлиқ эмаслиги сабабли электрон ресурснинг хавфсизлигини 30 дан 100% гача оширишга имкон беради.

12. Очик ресурсли платформага асосланган замонавий сайтларни бошкаришнинг ишлаб чиқилган ҳимоя усулларини амалга ошириш қуйидагиларга имкон берди: электрон ресурслардаги заифликлар мавжудлигига оператив холатни 1,1 баравар ошириш, веб-ресурсларнинг хавфсизлигини 25 %га ошириш, шунингдек, ахборот хавфсизлигини таъминлаш ва харажатларни камайтириш, хатоларга чидамлиликни 15% га оширишга эришилди.

13. Мосланувчан моделлар ва усуллар асосида электрон ресурсларни ахборот хавфсизлиги таҳдидларидан ҳимоя қилишга имкон берувчи "Adaptive Web Protector" дастурий воситаси яратилди. Ушбу дастурий таъминот барча кирувчи трафик фильтрланганлиги ва ушбу усул электрон ресурс ишлаб чиқиладиган тилга боғлиқ эмаслиги сабабли электрон ресурснинг хавфсизлигини 30 дан 100% гача оширишга имкон берди.

14. "Adaptive Web Protector" дастурий воситаси амалдиётда фойдаланилаётган электрон ресурсларда (aitm.uz, uzkadr.uz, skif.uz, mdcrm.uz, biocontrol.uz) синовдан ўтказилди, натижада ушбу дастурий восита муваффақиятли ҳимоя қилинди ҳамда оммабоп ахборот хавфсизлиги таҳдидларидан амалдаги электрон ресурсларини ҳимоя қилиш имкониятларини намойиш қилди.

НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.01 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КЕРИМОВ КОМИЛ ФИКРАТОВИЧ

АДАПТИВНЫЕ МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ РЕСУРСОВ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

05.01.05 - Методы и системы защиты информации. Информационная безопасность

АВТОРЕФЕРАТ ДОКТОРСКОЙ (DSc) ДИССЕРТАЦИИ ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент – 2020

Тема докторской диссертации по техническим наукам (DSc) зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2018.4.DSc/T243

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб странице (www.tuit.uz) и на Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный консультант:	**Хамдамов Рустам Хамдамович** доктор технических наук, профессор
Официальные оппоненты:	**Бекмуратов Тулкун Файзиевич** доктор технических наук, профессор, академик **Мусаев Мухаммаджон Махмудович** доктор технических наук, профессор **Опанасенко Владимир Николаевич** доктор технических наук, профессор
Ведущая организация:	**Национальный университет Узбекистана им. Мирзо Улугбека.**

Защита диссертации состоится «30» июня 2020 г. в 1500 часов на заседании научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер № 158). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «18» июня 2020 года.
(протокол рассылки № 13 от «17» августа 2020 г.).

Ш.Х. Фазилов
Зам. председателя научного совета по присуждению учёных степеней, д.т.н., профессор

Ф.М. Нуралиев
Ученый секретарь научного совета по присуждению учёных степеней, д.т.н., доцент

С.К. Ганиев
Председатель научного семинара при научном совете по присуждению ученых степеней, д.т.н., профессор

ВВЕДЕНИЕ (аннотация диссертации доктора наук (DSc))

Актуальность и востребованность темы диссертации. В мире особое внимание уделяется обеспечению безопасности электронных ресурсов и веб приложений. Разработка систем защиты электронных ресурсов, а также их применение для защиты автоматизированных систем для государственных организаций (министерства, ведомства, крупные компании), банковской сферы (государственные и частные), электронной коммерции (интернет магазины, платежные системы), различных производственных и коммерческих предприятий, информационно-образовательных ресурсов (дистанционное обучение, онлайн библиотеки) и других сферах имеет огромное значение, как для самого ведомства, так и для государства в целом. На сегодняшний день разработаны и исследованы различные методы защиты электронных ресурсов, в частности, методы на основе шаблонов, обнаружения аномалий и поведенческого анализа. Проблеме защиты электронных ресурсов уделяется большое внимание в таких странах как: США, Южная Корея, Украина, Япония, Российская Федерация, Индия и других.

В мире ведутся научные исследования, направленные на разработку моделей и методов, используемых для обеспечения защиты электронных ресурсов от угроз информационной безопасности. Несмотря на это существующие системы защиты электронных ресурсов основаны на методе шаблонов, который позволяет обнаруживать и защищать только угрозы имеющиеся в базе данных. Имеет место ряд проблем выявления и обнаружения угроз: зависимость существующих методов от отдельных эмпирических характеристик, приводящих к большому числу ложных срабатываний системы; узкий диапазон выявляемых известных угроз; невозможность определения новых угроз с неизвестными параметрами. В этом аспекте необходима разработка адаптивных методов, моделей, установление причинно-следственного анализа показателей защищенности. А также создание программного обеспечения, легкого в установке на серверной площадке, удобного в использовании и эффективном в работе.

В нашей республике особое внимание уделяется внедрению информационных технологий во многие сферы деятельности, в том числе, проведению научных исследований по разработке моделей и методов защиты информации. В стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017 - 2021 годах определены такие задачи, как «...внедрению информационно-коммуникационных технологий в экономику, социальную сферу, системы управления»[1]. Для реализации этих задач важными вопросами являются разработка адаптивных моделей и методов защиты электронных ресурсов на основе сигнатурного и поведенческого анализа.

[1] Указ Президента Республики Узбекистан от 7 февраля 2017 года №УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

Данное диссертационное исследование в определенной степени служит выполнению задач, предусмотренных в указе Президента Республики Узбекистан №УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», в постановлении Президента Республики Узбекистан от 29 августа 2017 года №ПП-3245 «О мерах по дальнейшему совершенствованию системы управления проектами в сфере информационно-коммуникационных технологий», в постановлении Президента Республики Узбекистан от 21.11.2018 г. №ПП-4024 "О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты", постановлении Кабинета Министров Республики Узбекистан от 05.09.2018 г. №ПКМ-707 "О мерах по совершенствованию информационной безопасности во всемирной информационной сети Интернет".

Соответствие исследования с приоритетными направлениями развития науки и технологий республики. Данное исследование выполнено в соответствии приоритетного направления развития науки и технологий республики IV. «Развитие информатизации и информационно-коммуникационных технологий».

Обзор научных исследований по теме диссертации. Научные исследования, направленные на разработку моделей защиты и обнаружения угроз информационной безопасности в электронных ресурсах осуществляются в ведущих научных центрах и высших образовательных учреждениях мира, в том числе, IBM Cyber Security Center of Excellence, Open Web Application Security Project, Information Security Research Association, SRI internation, Norwegian University of Science and Technology (Норвегия), University of South Wales (Великобритания), The University of Oxford (Великобритания), New Hampshire University (США), Seoul National University (Южная Корея), Asahi Kasei Microsystems (Япония), Московский Государственный Университет (Россия), «Центр технического содействия» государственное унитарное предприятие (Узбекистан).

В результате исследований, проведенных в мире по методам и моделям защиты электронных ресурсов от угроз информационной безопасности получены ряд научных результатов, в том числе: создана международная классификация угроз информационной безопасности (Open Web Application Security Project, США); разработаны методы безопасной разработки приложений на основе биометрической аутентификации, а также применяются методики когнитивной кибербезопасности (IBM Cyber Security Center of Excellence, США); учеными Сеульского национального университета разработаны модели анализа Web приложений на основе методов шаблонов (Seoul National University, Южная Корея); на основе анализа практического применения разработаны методы защиты Web приложений на основе модуля апаче mod_security (Московский Государственный Университет, Россия; University of South Wales, Великобритания).

В мире проводятся исследования по ряду приоритетных направлений по разработке моделей и методов выявления уязвимостей в Web приложениях, развитию и обновлению международной классификации уязвимостей Web приложений, созданию моделей выявления аномалий при работе в Web приложений, совершенствуются методики тестирования Web приложений на возможность проникновения и взлома.

Степень изученности проблемы. Теоретическим и практическим вопросам разработки систем информационной безопасности, методам и моделям защиты электронных ресурсов от угроз информационной безопасности посвящены многочисленные работы таких зарубежных ученых как: А.И. Галатенко, В.Н. Опанасенко, В.А. Герасименко, Д. Деннинг, П. Зегжда, А. Грушо, М.Р. Кострова, А.Р.Тихонова и других.

В Республике Узбекистан проблемы защиты информации, в частности, защита электронных ресурсов от угроз информационной безопасности изучены в исследованиях таких ученых, как: Т.Ф. Бекмуратов, М.М. Камилов, М.М. Арипов, М.М. Каримов, С.К. Ганиев, Р.Х.Хамдамов, Б.Ф. Абдурахимов, А.Х. Нишанов, А.В. Кабулов, А.А. Ганиев, О.П.Ахмедова, Р.И.Исаев и другие.

До настоящего времени не разработаны модели защиты электронных ресурсов от угроз информационной безопасности, которые имели бы под собой адекватную теоретическую основу.

Теоретические и практические исследования методов и моделей защиты электронных ресурсов от угроз информационной безопасности, безусловно, имеют важное значение для решения задач связанных с обеспечением безопасности электронных ресурсов.

Связь диссертационного исследования с планами научно-исследовательских работ научно-исследовательского учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках плана научно-исследовательских работ прикладных проектов в Ташкентском университете информационных технологий имени Мухаммада ал-Хорезмий: ЁА5-005 «Разработка методов и программного обеспечения для защиты государственных интернет ресурсов от угроз информационной безопасности, на основе интеллектуального анализа данных» (2015-2016); А5-075 «Разработка алгоритмов и программных средств обеспечения безопасности электронных сетевых ресурсов» (2015-2017); БВ-Атаб-2018-568 «Создание интеллектуальных программных систем управления информационными рисками для поддержки принятия решений по защите информации электронных ресурсов». (2018-2020); ЁБВ-Атех-2018-212 «Исследование и разработка методов и алгоритмов обеспечения безопасности информационных ресурсов в системах электронного правительства» (2018-2019).

Целью исследования является разработка адаптивных моделей и методов, основанных на сигнатурном и поведенческом анализе, для защиты электронных ресурсов от угроз информационной безопасности.

Задачи исследования:

сформировать признаковое пространство угроз информационной безопасности в электронных ресурсах;

создать базу данных сигнатур угроз информационной безопасности в электронных ресурсах;

разработать алгоритмы классификации угроз информационной безопасности в электронных ресурсах на основе параметрической идентификации;

разработать методы защиты электронных ресурсов используя брандмауэр для Web приложений;

разработать адаптивные модели параметрической идентификации, позволяющие выявлять угрозы информационной безопасности в электронных ресурсах.

разработать методы и алгоритмы защиты электронных ресурсов от угроз информационной безопасности на основе языконезависимых решений;

разработка адаптивной модели защиты электронных ресурсов от угроз информационной безопасности на основе поведенческого анализа;

разработать программное средство, осуществляющее защиту электронных ресурсов от угроз информационной безопасности.

Объектом исследования являются процессы обеспечения безопасности электронных ресурсов и веб приложений.

Предметом исследования являются модели, методы и алгоритмы защиты электронных ресурсов от угроз информационной безопасности.

Методы исследования. В работе используются методы защиты информации и методы интеллектуального анализа данных: метод шаблонов для исходного описания признаков, алгоритмический метод создания признаков в пространстве исходного описания, метод защиты электронных ресурсов от атак типа SQL инъекции и XSS при помощи технологии брандмауэра для Web приложений, а также алгоритмы классификации угроз информационной безопасности в электронных ресурсах на основе параметрической идентификации.

Научная новизна исследования заключается в следующем:

создано признаковое пространство и база данных сигнатур угроз информационной безопасности в электронных ресурсах, основанная на взаимодействии таблицы объект-признак;

разработаны алгоритмы классификации угроз информационной безопасности в электронных ресурсах, основанные на методах параметрической идентификации;

разработаны методы защиты электронных ресурсов от атак типа SQL (Structured Query Language) инъекции и XSS (Cross-Site Scripting), основанные на технологии брандмауэра для веб приложений;

разработаны адаптивные модели защиты электронных ресурсов, основанные на сигнатурном и поведенческом анализе;

разработаны методы и алгоритмы защиты электронных ресурсов от угроз информационной безопасности, основанные на языконезависимых решениях.

Практические результаты исследования заключаются в следующем:

разработаны алгоритмы классификации угроз информационной безопасности в электронных ресурсах на основе параметрической идентификации, позволяющие идентифицировать известные угрозы информационной безопасности в электронных ресурсах;

разработаны методы защиты электронных ресурсов используя брандмауэр для Web приложений, позволяющие защищать электронные ресурсы от известных и неизвестных угроз информационной безопасности;

разработаны адаптивные модели параметрической идентификации, позволяющие защищать электронные ресурсы от неизвестных видов угроз информационной безопасности.

Достоверность результатов исследования обосновывается корректностью постановки задачи на основе адаптивных методов параметрической идентификации, строгостью математических выкладок, использованием обоснованных методов решения, исследованием сходимости вычислительных алгоритмов и методов на основе технологии брандмауэра для Web приложений.

Научная и практическая значимость результатов исследования.

Научная значимость результатов диссертационной работы заключается в разработке адаптивных моделей и методов защиты электронных ресурсов от угроз информационной безопасности, основанной на принципах, методах адаптивной параметрической идентификации. Также были разработаны методы и алгоритмы защиты электронных ресурсов от угроз информационной безопасности на основе языконезависимых решений

Практическая значимость работы заключается в том, что предлагаемые модели и методы легли в основу разработки соответствующего программного обеспечения, которое позволило эффективно защищать электронные ресурсы созданных на любых системах управления. Данные модели и методы позволили защищать электронные ресурсы от неизвестных видов угроз информационной безопасности.

Внедрение результатов исследования. На основе полученных научных результатов по обеспечению защиты электронных ресурсов от угроз информационой безопасности:

признаковое пространство и база данных сигнатур угроз информационной безопасности в электронных ресурсах, основанная на взаимодействии таблицы объект-признак, и разработанное на их основе программное средство внедрены в деятельность Центра информационной безопасности и содействия в обеспечении общественного порядка (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 марта 2019 года 33-8/1922). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 1,5 раза, а также увеличить защищённость веб ресурсов на 12%.

методы обеспечения защиты электронных ресурсов от атак типа SQL инъекции и XSS, основанные на технологии брандмауэра для веб

приложений, и разработанное на их основе программное средство внедрены в деятельность филиала «ТТТ» АК «Узбектелеком» (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 марта 2019 года 33-8/1922). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 1,7 раза, а также увеличить защищённость веб ресурсов на 18%.

алгоритмы классификации угроз информационной безопасности в электронных ресурсах, основанные на методах параметрической идентификации, а также методы защиты электронных ресурсов на основе технологии брандмауэра для веб приложений, и разработанное на их основе программное средство внедрены в деятельность дирекции обеспечения информационной безопасности и информационного развития АО "Узбекистон темир йуллари" (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 марта 2019 года 33-8/1922). Использование результатов научного исследования позволило уменьшить время реакции на наличие уязвимостей в электронных ресурсах на 50%, а также увеличить защищённость веб ресурсов на 50%.

методы и алгоритмы защиты электронных ресурсов от угроз информационной безопасности, основанные на языконезависимых решениях, и разработанное на их основе программное средство внедрены в деятельность ООО "SKIF" (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 марта 2019 года 33-8/1922). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 2 раза, а также увеличить защищённость веб ресурсов на 30%.

признаковое пространство и база данных сигнатур угроз информационной безопасности в электронных ресурсах, основанная на взаимодействии таблицы объект-признак, а также алгоритмы классификации угроз информационной безопасности в электронных ресурсах на основе параметрической идентификации, и разработанное на их основе программное средство внедрены в деятельность ООО "SMART SOFTWARE" (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 30 марта 2019 года 33-8/1922). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 2,5 раза, а также увеличить защищённость веб ресурсов на 50%.

методы защиты электронных ресурсов от атак типа SQL (Structured Query Language) инъекции и XSS (Cross-Site Scripting), основанные на технологии брандмауэра для веб приложений, а также адаптивные модели защиты электронных ресурсов, основанные на сигнатурном и поведенческом анализе и разработанное на их основе программное средство внедрены в деятельность ООО "SOFTWARE DESIGN" (справка Министерства по

развитию информационных технологий и коммуникаций Республики Узбекистан от 30 марта 2019 года 33-8/1922). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 1,1 раза, а также увеличить защищённость веб ресурсов на 25%.

Апробация результатов исследования. Основные теоретические и практические результаты диссертационной работы докладывались и обсуждались на 3 международных и 2 республиканских конференциях.

Опубликованность результатов исследования. Опубликованность результатов исследования. Основные результаты исследования опубликованы в 29 научных работах, из которых 18 опубликованы в журналах, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, в том числе 3 в зарубежных и 15 в республиканских журналах, а также получены 4 свидетельств об официальной регистрации программы для ЭВМ.

Объем и структура диссертации. Структура диссертации состоит из введения, пяти глав, заключения, списка использованной литературы, приложений. Объем диссертации составляет 194 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обоснована актуальность и востребованность темы диссертации, приводится соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, сформулирована цель и задачи, объект и предмет исследования, изложена научная новизна, практические результаты исследования, обоснована достоверность полученных результатов, раскрывается теоретическая и практическая значимость результатов исследования, приведены внедрения результатов исследования, сведения об опубликованности результатов и структуре диссертации.

В первой главе диссертации «**Анализ современных методов, моделей и средств защиты электронных ресурсов от угроз информационной безопасности**» дается анализ современного состояния популярных видов угроз ИБ, изучены тенденции развития и современные методы и модели защиты электронных ресурсов от угроз ИБ. Описаны существующие программные средства, позволяющие защитить электронные ресурсы от угроз ИБ. Показаны наиболее распространённые угрозы, такие так:

- удаленный запуск кода на сервере;
- SQL – инъекции;
- XPath – инъекции;
- удаленный запуск файла на сервере;
- запуск локального файла;
- угроза ИБ вида XSS;

- угроза ИБ вида CSRF.

Рассмотрены существующие модели защиты электронных ресурсов от угроз ИБ, было выявлено, что существуют 2 вида моделей, это сигнатурные (шаблонные) и модели анализа поведения пользователя и системы (поведенческие). Сигнатурные модели защиты ЭР от угроз ИБ включают в себя 3 вложенные модели:

- Модель шаблонного поиска,
- Модель анализ текущего состояния,
- Биологические модели.

Алгоритм работы поведенческих моделей заключается в поиске не соответствий между нормальным поведением системы и текущим состоянием. При нахождении не соответствий, такая ситуация рассматривается как найденная угроза ИБ.

Во второй главе диссертации «Адаптивные модели и алгоритмы защиты электронных ресурсов от угроз информационной безопасности» приведена концепция адаптивной защиты информационных систем от угроз информационной безопасности. Также во второй главе предложен алгоритм обнаружения атаки по инъекции SQL с помощью функции распознавания, и оценка эффективности предложенного алгоритма с помощью искусственных данных. Также, предложена модель информационного объекта. На основе данной модели был построен алгоритм обнаружения XSS атак на веб приложения, принимая во внимание частоту появления и коэффициент важности символов, участвующих при построении входящих запросов. Разработана адаптивная модель защиты электронных ресурсов от угроз информационной безопасности на основе обнаружения аномалий.

В параграфе 2.1 предложена концепция адаптивной защиты электронных ресурсов от угроз информационной безопасности. Рассмотрены четыре уровня, которые включают в себя электронный ресурс:

1. Уровень веб приложения, то есть данный уровень обрабатывает связи с пользователями. Например, электронный ресурс портала по продаже бытовой техники, различные сайты организаций и т.д.
2. Уровень работы с базами данных, то есть данный уровень обрабатывает данные системы, а также осуществляет хранение информации Например: Mysql, Postgresql.
3. Уровень работы с ОС, то есть данный уровень отвечает за все компоненты системы, такие, как веб сервер, интерпретатор, само ядро системы и т.д.
4. Уровень работы с сетью, данный уровень отвечает за сетевое взаимодействие пользователей и электронного ресурса.

На любой из вышеперечисленных элементов может совершена атака, которая в конечном счете затронет электронный ресурс.

Адаптивный механизм позволит выявлять и принимать решения на угрозы ИБ, при помощи хорошо отлаженных и управляемых средств.

Адаптивная безопасность электронного ресурса включает в себя следующие компоненты:

- Алгоритмы классификации угроз ИБ,
- Адаптивные модели защиты электронных ресурсов от угроз ИБ,
- Адаптивные методы защиты электронных ресурсов от популярных угроз ИБ.

Рис 1. Схема взаимодействия электронного ресурса со всеми элементами инфраструктуры

Адаптивный элемент безопасности отвечает за изменение функциональности анализа защиты электронного ресурса, передавая и обновляя данные о новых угрозах ИБ. Например, обновление сигнатур, которые позволяют обнаруживать угрозы ИБ.

Адаптивный элемент также может осуществлять оповещение на определенные действия, а именно:

- Осуществление оповещения в виде sms, по telegram либо по email;
- Обнаружение атак и их моментальная блокировка;
- Разработка рекомендаций по устранению той или иной угрозы ИБ.

В разделе 2.2.1 показаны алгоритмы классификации угроз информационной безопасности на основе сигнатурного анализа. Для классификации угроз ИБ в электронных ресурсах был разработан математический способ идентификации атак с помощью ограниченной снизу функции, которая зависит от входной строки. Для построения такой функции были использованы специальные знаки и ключевые слова, которые часто встречаются в построении атак злоумышленников.

Рассмотрим работу алгоритма классификации на основе популярных угроз ИБ в электронных ресурсах вида SQL инъекция XSS.

Угроза ИБ вида SQL инъекция выполняется посредством сигнатуры, которая введена через форму на веб-странице либо другим способом, позволяющим менять входящие параметры. Рассмотрим пример SQL инъекции. Запросы отправляется на form.php. В данном файле, запишется следующее:

$test = $_GET['test'];

$query = "SELECT * FROM userlist WHERE user='$test";

Здесь делается выборка данных по значению переменной $test. После этого посылается запрос с кавычкой:

site.uz/index2.php?user=KamilPHP'

Если по выполнения данного запроса выходит ошибка, то уязвимость вида SQL инъекция имеет место быть. Далее определяется, является ли вводимая строка атакой или нет, используя группу из этих символов. Для этого необходимо разработать алгоритм, который исходя из специальных символов будет определять, является ли входящая строка нормальным запросом либо атакой.

Для определения SQL инъекции вводится характеристики атак SQL инъекций с помощью специальных символов из таблицы 1 и специальных ключевых слов из таблицы 2. Пусть наблюдается некоторая входная строка L и пусть $x_1, x_2, \dots x_{20}$ частота появления в L специальных знаков из таблицы 1 и пусть $x_{21}, x_{22}, \dots x_{30}$ являются частотой появления специальных ключевых слов из таблицы 2 , x_{31} частота появления всех букв и цифр 0,1,2,...,9 в строке L. С точки зрения определения атак SQL инъекций обычные буквы $a, b, \dots z$ и цифры $0, 1, \dots , 9$ не играют важную роль. Поэтому будем считать, что частота появления всех этих букв и цифр в наблюдаемой строке L равно 1, т.е. $x_{31} = 1$. Таким образом, любую строку L можно определить с помощью характеристик следующим образом: $L = x_1, x_2, \dots x_{20}, x_{21}, \dots, x_{30}, x_{31}$, как элемент некоторого фазового пространства X. В построении атак SQL инъекций часто используются специальные символы и специальные ключевые слова, которые приведены в следующих таблицах.

Таблица 1

Объект признак(специальных символов)

Переменная	Символ
u_1	Пробел
u_2	Точка-запятая(;)
u_3	Апостроф(')
u_4	Правая скобка())
u_5	Левая скобка(()
u_6	Правая фигурная скобка (})
u_7	Левая фигурная скобка ({)
u_8	Правая квадратная скобка (])
u_9	Левая квадратная скобка([)
u_{10}	Диез(#)
u_{11}	Процент (%)
u_{12}	Кавычка (")
u_{13}	Амперсанд (&)
u_{14}	Обратная косая (\)
u_{15}	Вертикальная линия (|)
u_{16}	Знак равенства (=)
u_{17}	Больше чем (>)
u_{18}	Меньше чем (<)
u_{19}	Звездочка (*)
u_{20}	Косая черта (/)

Таблица 2

Объект признак (специальных ключевых слов)

Переменная	Ключевые слова
u_{21}	and
u_{22}	or
u_{23}	union
u_{24}	where
u_{25}	limit
u_{26}	group by
u_{27}	select
u_{28}	\'
u_{29}	hex
u_{30}	substr

Алгоритм определения. Из определения L видно, что любой элемент L из построенного пространства X лежит на гиперплоскости $\Gamma = \{L = (x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}) : x_{31} = 1\}$. Используя данное уравнения гиперплоскости, можно предположит, что чем больше частота появления специальных знаков и ключевых слов во входной строке, тем очевиднее становится близость входной строки L к атакам SQL инъекций. Поэтому, функция определения атаки должна быть возрастающей по переменным $x_1, x_2, \dots, x_{20}, x_{21}, \dots x_{30}$, и убывающей по переменной x_{31}. Исходя из этого предлагаем следующую возрастающую по $x_1, x_2, \dots, x_{20}, x_{21}, \dots x_{30}$ функцию

$$f(L) = f(x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}) = \frac{\sum_{i=1}^{30} x_i}{\sum_{i=1}^{30} x_i + x_{31}}$$

для определения атак SQL инъекций. Частота появления всех остальных букв и цифр 0,1, 2,.... 9 в строке L равно 1, то из последнего равенства получим

$$f(L) = f(x_1, x_2, \dots, x_{20}, \dots x_{30}, x_{31}) = \frac{\sum_{i=1}^{30} x_i}{\sum_{i=1}^{30} x_i + 1} \qquad (1)$$

Данная функция имеет следующее свойство: 1) $0 \le f(L) < 1$ для всех $L \in \Gamma$

2) для атак SQL инъекций минимальное значение функции снизу ограничена числом 1/2.

Таким образом, если входная строка L является атакой SQL инъекции, то эта строка по крайней мере должна содержать один специальный символ из таблицы 1 или одно ключевое слово из таблицы 2. Поэтому $\sum_{i=1}^{30} x_i \ge 1$ и так как функция $f(L)$ является возрастающей по каждому из переменных x_i её минимум при $\sum_{i=1}^{30} x_i \ge 1$ достигается в точке L_0, для которого $\sum_{i=1}^{30} x_i = 1$.

Таким образом, если L произвольная строка и $f(L) \ge 1/2$, то L возможно является атакой SQL инъекции, или же $f(L) < 1/2$, то тогда входная строка возможно является нормальной, если при построении атак SQL инъекций используются специальные ключевые слова из таблицы 2. Поэтому функцию (1) можно использовать для распознавания нормальных строк и атак SQL инъекций, построенных с помощью специальных символов и ключевых слов.

Таким образом, если L произвольная строка, содержащая минимум 2 специальных символов из таблицы 1, то $f(L)\geq 2/3$, и L возможно является атакой SQL инъекции, или же $f(L)<2/3$, то тогда входная строка, возможно является нормальной, если при построении атак SQL инъекций используются только специальные символы из таблицы 1. Поэтому функцию (1) можно использовать для распознавания нормальных строк и атак SQL инъекций, построенных с помощью специальных символов из таблицы 1 и специальных ключевых слов из таблицы 2.

В обоих случаях используя функцию (1) имеем критерий качества для определения угроз. В нашем случае границей разпознающей функции (1) является рациональное число 1/2. Таким образом, если строка L содержить хотя бы один специальный знак или же одно ключевое слово, то условие $f(L)\geq 1/2$ достаточно для определения угрозы.

Таблица 3

Образцы строк содержание SQL инъекции

Номер	Строки атаки
1	id=1'
2	KamilPHP'
3	KamilPHP'%20--%20test
4	1 UNION SELECT 1,2

Таблица 4

Образцы нормальных строк

Номер	Нормальные строки
1	Test
2	password
3	kamil@
4	@kamil
5	{(1%2)+(3/4)}/5}
6	&temptest(URL){ width,height }

Вычисление степени важности ключевых слов. Для определения степени важности специальных знаков из таблицы 1 проведены экспериментальные вычисления исходя из 39 атак по инъекции SQL. При этом, была использована следующая формула:

$K_B = \frac{K_U}{K_N}$, где K_B - степень важности специального знака U, который в дальнейшем будет называться коэффициентом важности знака U, K_U- количество атак по SQL инъекции L, при построения которых используется специальный знак u, K_N - общее количество атак по SQL инъекций.

Далее, используя введенные обозначения, определим входную строку, как вектор с числовыми координатами:

$$L = (K_U, x_1, K_U, x_2, \ldots, K_{U_{30}} x_{30}, K_{U_{31}} x_{31}) \qquad (2)$$

Такое определение входной строки отличается от предыдущего тем, что координаты входной строки (2) имеют различные значения, отличные от единицы. Поэтому разные входные строки имеют различие в координатах. Но если в пространстве X определено понятие длины в каком то смысле, то некоторые входные строки могут иметь одинаковую длину. Этот факт не помешает различить входные строки. Отличительной чертой входной строки-атаки по SQL инъекций определенной согласно (2) является то, что она имеет только неотрицательные координаты и поэтому если длина строки строго положительна, то это строка возможно будет близка к атаке по SQL инъекций.

Таким образом, можно построить новую функцию распознавания, используя определение (2) для входной строки. Тогда функция распознавания определяет входную строку более точно чем (1), так как в этом случае при построении функции распознавания учитывается коэффициент важности всех знаков из таблиц 1,2. Но при этом, важно отметить, что для определения коэффициента важности каждого знака необходимо провести экспериментальные вычисления над большим количеством атак SQL инъекций (например, 500-600 штук атак SQL инъекций). И тогда коэффициенты важности каждого знака будет неизменной почти для всех атак SQL инъекций. Учитывая этот факт построим новую функцию для определения атак SQL инъекций:

$$f_K(L) = f\left(x_1, x_2, \dots, x_{20}, x_{21}, \dots, x_{31}\right) = \frac{\sum_{i=1}^{30} K_U.x_i}{\sum_{i=1}^{30} K_U.x_i+1} \qquad (3)$$

Теперь для определения статуса входной строки (2) вместо функции (1) можно использовать функцию (3). Здесь также как и выше можно определить нижнюю границу функции (3) для выявления атак SQL инъекций.

В таблице 5 можно видеть результаты эксперимента.

Алгоритм распознавания состоит из следующих шагов:

1-шаг. Используя реальную входную строку определяется объект L согласно (2).

2-шаг. Вычисляется значение функции (3).

3-шаг. Определяется минимальное значение функции (3).

4-шаг. Сравнивая значение функции (3) с её минимальным значением определяется статус входной строки.

Видно, что все функции определения статуса входных строк зависят от моделирования информационного объекта (входных строк). Поэтому очень важной задачей является принцип формализации определения входной строки. Решение этой задачи во многом определяет и методы решения распознавания информационных объектов.

На основе данного алгоритма, происходит определение угрозы ИБ вида XSS.

В разделе 2.2.1 показана разработка адаптивной модели защиты электронных ресурсов от угроз информационной безопасности на основе поведенческого анализа.

Таблица 5

Определение степени важности для спец. знаков y

	Степень важности для специальных знаков y
=	0.4872
%	0.2051
'	0.6923
*	0.0769
/	0.0513
]	0.0256
[	0.0257
{	0
}	0
&	0
\	0
#	0.0513
"	0
!	0
<	0.0256
>	0.0255
(	0.1538
)	0.1795
;	0
Пробел	0.7949

Выявлены HTTP/HTTPS запросы, которые могут указывать на наличие угрозы ИБ.

1. Запросы, в которых содержаться вредоносные символы в параметре URL;
2. Запросы, которые запрашивают не существующие страницы электронного ресурса;
3. Запросы, в которых отсутствует или искажен параметр User-Agent;
4. Запросы, в которых искажен или содержит вредоносный код параметр Referer;
5. Запросы, в которых искажен или содержит вредоносный код параметр Cookie;
6. Запросы, в которые длина параметров превышает указанные ограничения;

На примере 1 запроса (запросы, в которых содержаться вредоносные символы в параметре URL) покажем разработанные критерии эталонов.

Приведем разработанные критерии, эталонного URL:

K_1 – Длина URL, которая настраивается под конкретный электронный ресурс;

K_2 – Отсутствие определенных специальных символов, свидетельствующих о наличии угрозы ИБ;
K_3 – Отсутствие определенных специальных слов, свидетельствующих о наличии угрозы ИБ.

Ниже приведена схема адаптивной модели:

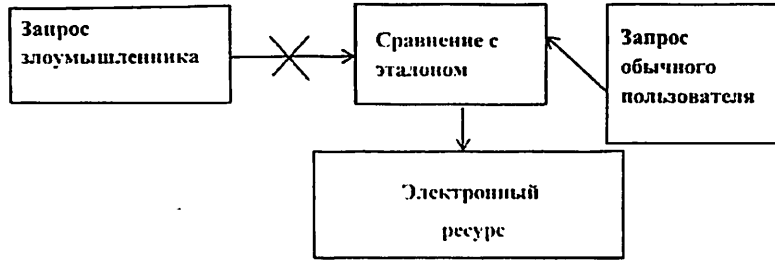


Рис 2. Схема работы адаптивной модели

Данные параметры являются регулируемыми и могут адаптироваться под каждый электронный ресурс

Разработана схема обнаружения и защиты электронного ресурса, на основе анализа и идентификации параметра URL:

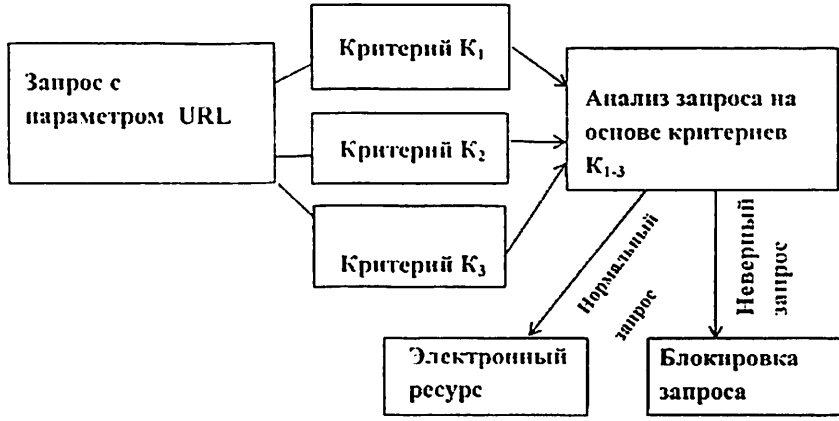


Рис. 3 Схема обнаружения и защиты электронного ресурса, на основе анализа и идентификации параметра URL

Для каждого вредоносного запроса разработаны критерии для определения данного вида запросов. Общее количество критериев 17. Если запрос к электронному ресурсу $\in K_n$, где n от 1 до 17, то данный запрос будет пропущен к электронному ресурсу, иначе заблокирован.

Третья глава диссертации **«Методы и алгоритмы защиты электронных ресурсов от угроз информационной безопасности на основе**

языконезависимых решений» посвящена методам блокирования XSS на основе сервис ориентированной архитектуры, а также приведены принципы оценки риска ИБ при несанкционированном доступе к электронным ресурсам компьютерной сети. Показана структура базы данных для решения задач оценки рисков ИБ компьютерной сети.

Параграф 3.1 посвящён разработке метода блокирования угроз ИБ вида XSS, в основе которого лежит возможность защиты электронных ресурсов от угроз ИБ вида XSS при помощью XML и XSD. Это включает в себя создание XML-документа на основе всех элементов управления формы, представленных пользователем. Данный XML-документ будет проверен на соответствие схеме на стороне сервера. Любой вредоносный сценарий приведет к созданию недопустимого или неправильно сформированного XML-файла, и таким образом, не позволит пользователю отправить вредоносные сценарии.

В параграфе 3.2 приведен метод защиты базы данных на основе брандмауэр веб-приложений. Механизм работы метода основан на работе прокси, то есть, что принимаемые от клиента запросы на SQL-выражения будут сначала отправлены на разработанный брандмауэру, нежели самому серверу базы данных (БД). Брандмауэр (БМ) анализирует запрос: запросы, считающиеся странными, блокируются брандмауэром и клиенту возвращается пустой результат. В противном случае, он вызовет сервер базы данных для выполнения запроса.

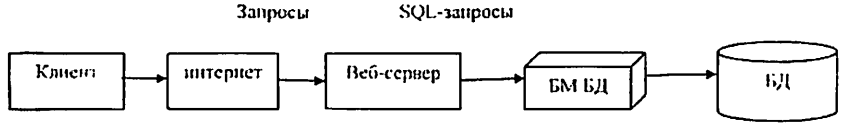


Рис. 4 Архитектура брандмауэра для базы данных

Параграф 3.4 посвящён методу оценки риска информационной безопасности компьютерной сети по результатам проведенного анализа признаков уязвимости и защиты элементов информационной системы.

Осуществлено формирование пространства признаков защиты информации и приведен анализ возможных вариантов угроз несанкционированного доступа к электронным ресурсам компьютерной сети. Приведены решения по снижению рисков информационной безопасности.

Четвертая глава диссертации **«Методы защиты электронных ресурсов от угроз информационной безопасности на основе брандмауэра веб-приложений»** посвящена методам защиты электронных ресурсов, используя брандмауэр на основе технологии XML. Также рассмотрены проблемы проектирования архитектуры брандмауэра и политики фильтрации. Успешно выполнены три политики фильтрации, а именно фильтрация размера

сообщения, синтаксический анализ и проверка XML-схемы были протестированы с действительными и недопустимыми сообщениями SOAP.

В параграфе 4.1 показана концепция построения брандмауэра веб-приложений. Для построения брандмауэра веб-приложений были разработаны меры по защите от популярных угроз ИБ, таких как SQL-инъекция, межсайтовый скриптинг (XSS), отказ в обслуживании (DOS). Разработана структура брандмауэра веб-приложений, состоящая из трех подсистем:

Рис. 5 Структура брандмауэра веб-приложений

Параграф 4.2 посвящён методу защиты электронных ресурсов, используя брандмауэр на основе технологии XML.

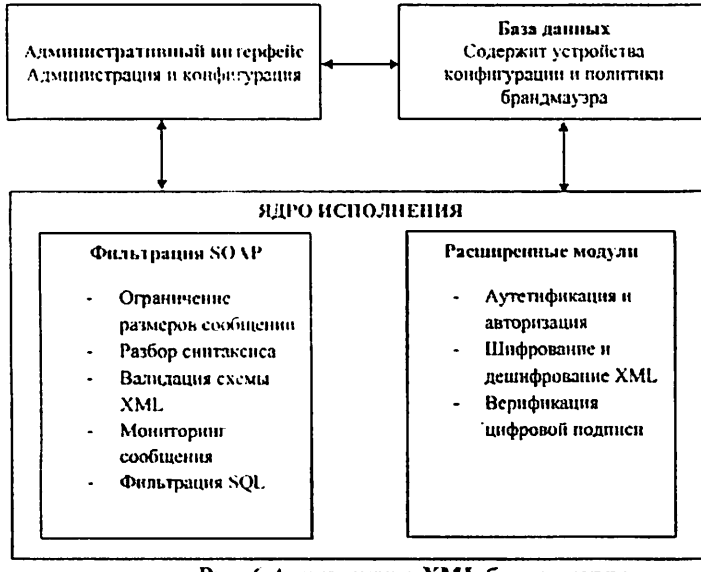


Рис. 6 Архитектура XML брандмауэра

Разработаны политики фильтрации для предотвращения различных типов атак на веб-сервисы, такие как:

- ограничение размера сообщении,
- синтаксический разбор,
- проверка схемы XML,
- мониторинг сообщений,
- SQL-фильтрация.

В параграфе 4.3 изложен метод защиты электронных ресурсов, используя брандмауэр веб приложений.

Для защиты электронных ресурсов от угроз ИБ был разработан метод, использующий механизм брандмауэра веб приложений, который разворачивается для обеспечения повышенного уровня безопасности обнаружения и предотвращения атак, до достижения этих атак электронных ресурсов. Это обеспечивает защиту от целого спектра атак на электронные ресурсы, позволяет мониторить HTTP трафик и анализировать небольшие изменения или постоянное состояние в режиме он-лайн.

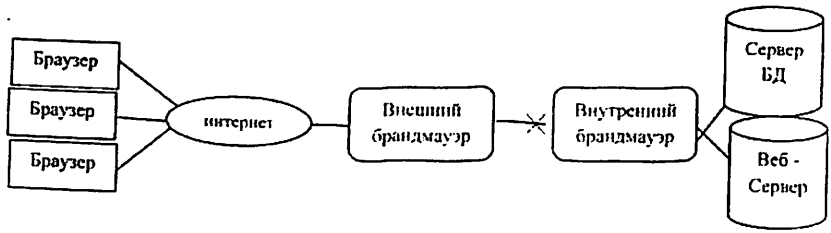


Рис. 7 Схема организации брандмауэра для электронных ресурсов

Брандмауэр для электронных ресурсов развертывается как часть структуры веб-сервера или как обратный прокси-сервер в сети. На рисунке 7 представлена схема организации брандмауэра для электронных ресурсов.

Для обеспечения защиты необходимо разработать правила. Преимуществом использования набора правил является то, что они не нуждаются в сигнатурах и могут обеспечить защиту от неизвестных видов угроз ИБ, часто находимых в электронных ресурсах.

Рассмотрим данные правила:

- защита HTTP - выявление нарушений HTTP протокола и определение для локального пользования политики;
- защита от обычных веб-атак - обнаружение типичных атак на безопасность веб-приложения;
- защита от автоматики - обнаружение ботов, "червей", сканеров и другой вредоносной деятельности;
- защита от трояна - обнаружение доступа к троянским коням;
- сокрытие ошибок - искажение сообщений ошибок, посылаемых серверу.

Для обеспечения защиты электронных ресурсов была разработана комплексная архитектура система обеспечения безопасности электронных ресурсов.

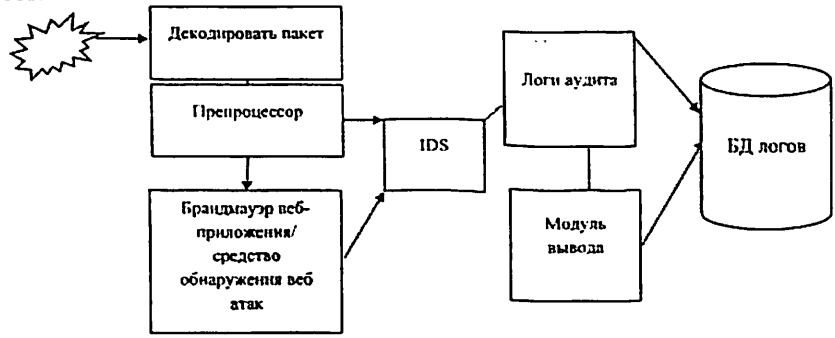


Рис. 8 Архитектура разработанной системы

Были разработаны два механизма блокирования данных угроз ИБ:

- на основе файла .htaccess;
- на основе внедрения в index файл кода подключения модуля защиты от угроз ИБ.

Рассмотрим более подробно каждый из механизмов:

На основе файла .htaccess. Файл .htaccess необходим для конфигурирования веб сервера со стороны разработчика электронного ресурса. И как следствие изменения конфигурацию этого файла, можно менять работу электронного ресурса. Данный файл располагается в корне электронного ресурса, а радиус его работы действует на весь электронный ресурс, включая все каталоги и подкаталоги. Все запросы которые идут к электронному ресурсу сначала идут на обработку в файл .htaccess, а уже потом запросы либо проходят либо блокируется.

Рассмотрим схему работы брандмауэра веб приложений на основе htaccess.

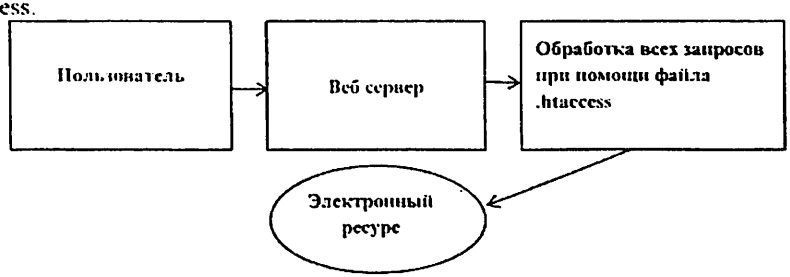


Рис. 9 Схема работы брандмауэра веб приложений на основе .htaccess

В файле .htaccess определяется следующие виды критериев, по которым будут защищен электронный ресурс:

- выставляется главная страница на ошибки 404 и 403;
- отключается опасные функции языка PHP;
- запрещается любые виды запросов, кроме POST и GET;
- блокируется доступ к файлам с конфигурацией и паролями от электронного ресурса;
- запрещается доступ к системным файлам, в которых могут содержаться пароли доступа;
- блокируется доступ к сайту из черного списка;
- блокируется доступ к сайту с неверным UserAgent'ом;
- защита от SQL инъекций и межсайтового выполнения сценариев;
- блокируется доступ к системным каталогам.

Рассмотрим пример работы защиты от SQL инъекций:

RewriteEngine On

RewriteCond %{THE_REQUEST} union[^\(]\(*

RewriteCond%{THE_REQUEST}(.<|>|'|"|\).*(/*|union|select|insert|drop|delete|update|create|alter|script|encode)*

На основе внедрения в index файл кода подключения модуля защиты от угроз ИБ. Электронный ресурс может работать со многими веб серверами, но файл htaccess доступен только на веб сервере apache (наиболее популярном веб сервере). Для того, чтобы охватить и другие веб сервера разработан механизм основы внедрения в index файл кода подключения модуля защиты от угроз ИБ.

Данный механизм основан на подключении в индексный файл библиотеки, которая анализирует все запросы.

Данный механизм позволяет без особых технических ресурсов защитить электронный ресурс от угроз ИБ, а также плюсом является возможность анализировать запросы, где используется SSL, потому что защита стоит на веб сервере самого электронного ресурса.

В пятой главе диссертации «**Апробация программных средств защиты электронных ресурсов от угроз информационной безопасности**» приведено программное средство Adaptive Web protector, разработанное на основе адаптивных моделей и методов, позволяющее защищать электронные ресурсы от угроз ИБ.

ЗАКЛЮЧЕНИЕ

На основе результатов проведенного исследования на тему «Адаптивные модели и методы обеспечения защиты электронных ресурсов от угроз информационной безопасности» представлены следующие основные выводы:

1.Обоснована целесообразность и перспективность разработки адаптивных моделей и методов защиты электронных ресурсов от угроз ИБ. Цели и задачи, поставленные в диссертационной работе, в полном объеме выполнены.

2. Предложена концепция адаптивной защиты электронных ресурсов от угроз информационной безопасности, что позволяет выработать меры по адаптивной защите ресурсов, используя как сигнатурный, так и поведенческий анализ.

3. Создан алгоритм обнаружения атаки по инъекции SQL с помощью функции распознавания, и оценку эффективности предложенного алгоритма с помощью искусственных данных. В предлагаемом алгоритме создан набор символов, который сочетается как с атакой, так и с нормальными обнаружениями, и с ранее известным порогом, используя примерные данные атакующих и нормальных строк. Данный алгоритм позволяет обнаруживать угрозы ИБ вида SQL инъекции на основе сигнатурного анализа.

Внедрение методов обеспечения защиты электронных ресурсов от угроз ИБ типа SQL инъекции и XSS позволило: увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 1,7 раза, увеличить защищённость web ресурсов на 18%, а также снизить затраты на обеспечение информационной безопасности и отказоустойчивости на 20%.

4. Разработана адаптивная модель защиты электронных ресурсов от угроз информационной безопасности на основе поведенческого анализа, данная модель позволяет защищать электронные ресурсы как от тех угроз ИБ, которые уже есть в базе, так и от новых видов угроз ИБ.

Внедрение созданного признакового пространства угроз информационной безопасности, алгоритмов классификации угроз информационной безопасности в электронных ресурсах позволило увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 2,5 раза, увеличить защищённость web ресурсов на 50% а также снизить затраты на обеспечение информационной безопасности и отказоустойчивости на 30%.

5. Проведен сравнительный анализ существующих моделей защиты электронных ресурсов с адаптивной моделью защиты электронных ресурсов. По результатам сравнительного анализа было установлено, что адаптивная модель имеет преимущества по количеству набранных баллов (9).

6. Разработан метод блокирования XSS на основе сервис ориентированной архитектуры, что позволяет обеспечить защиту электронных ресурсов, написанных на большинстве популярных языках программирования.

7. Разработаны принципы оценки риска ИБ, при несанкционированном доступе к электронному ресурсу компьютерной сети, основанные на распознавании признаков угроз несанкционированного доступа к электронным ресурсам компьютерной сети, что позволяет определить потенциальные риски для электронного ресурса.

8. Разработан метод защиты баз данных Web приложений от угроз ИБ, осуществлена реализация и оценка работы брандмауэра для баз данных.

Данный метод позволяет построить защиту баз данных на основе брандмауэра, это обеспечивает защиту данных от угроз ИБ вида SQL инъекция. Увеличивается защищённость электронных ресурсов от 30 до

100% в зависимости в какой платформе создан электронный ресурс. Внедрение методики обеспечения защиты таких популярных систем управления сайтами как Drupal, Wordpress, Joomla, а также механизма фильтрация запросов к Web узлу позволило: увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 2 раза, увеличить защищённость web ресурсов на 30%, снизить затраты на обеспечение информационной безопасности и отказоустойчивости на 30%.

9. Разработан метод выявления вирусов на страницах электронного ресурса, который позволяет обеспечить защиту электронного ресурса от вредоносного содержимого. Данный метод позволяет выявлять именно Web вирусы, которые распространяются среди Web приложений.

10. Предложена концепция построения брандмауэра Web-приложений, которая позволяет определить меры для разработки методов защиты электронных ресурсов на основе брандмауэра Web-приложений.

11. Разработан метод защиты электронных ресурсов на основе брандмауэр Web-приложений, используя технологию xml. также рассмотрены проблемы проектирования архитектуры брандмауэра и политики фильтрации. Успешно выполнены три политики фильтрации, а именно фильтрация размера сообщения, синтаксический анализ и проверка XML-схемы. Они были протестированы с действительными и недопустимыми сообщениями SOAP. Данный метод позволяет идентифицировать элементы атаки в сообщениях SOAP и блокировать сообщения. Таким образом, это может предотвратить различные атаки на Web-сервисы. Применение данного метода позволяет увеличить степень защищенности электронного ресурса от 30 до 100% за счет того, что весь входящий трафик проходит фильтрацию и данный метод не зависит от того, на каком языке разработан электронный ресурс.

12. Внедрение разработанных методов защиты современных систем управления сайтами, которые базируются на платформе Open source, позволило: увеличить оперативное реагирование на наличие уязвимостей в электронных ресурсах в 1.1 раза, увеличить защищённость web ресурсов на 25%, а также снизить затраты на обеспечение информационной безопасности и отказоустойчивости на 15%.

13. На основе адаптивных моделей и методов создано программное средство Adaptive Web protector, позволяющее защищать электронные ресурсы от угроз ИБ. Данное программное средство позволяет увеличить степень защищенности электронного ресурса от 30 до 100% за счет того, что весь входящий трафик проходит фильтрацию и данный метод не зависит от того на каком языке разработан электронный ресурс.

14. Проведена апробация работы программного средства Adaptive web protector на реальных электронных ресурсах (aitm.uz, uzkadr.uz, skif.uz, mdcrm.uz, biocontrol.uz), по результатам которой было установлено, что программное средства Adaptive web protector успешно защитило реальные электронные ресурсы от популярных угроз ИБ.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES
DSc.13/30.12.2019.T.07.01 AT TASHKENT UNIVERSITY OF
INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

KERIMOV KOMIL FIKRATOVICH

ADAPTIVE MODELS AND METHODS FOR PROTECTING ELECTRONIC RESOURCES FROM INFORMATION SECURITY THREATS

05.01.05 – Methods and systems of information protection. Information security

ABSTRACT OF THE DOCTORAL (DSc)
DISSERTATION OF TECHNICAL SCIENCES

Tashkent – 2020

The theme of doctoral (DSc) dissertation of technical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2018.4.DSc/T243.

The dissertation has been prepared at Tashkent University of Information Technologies.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website (www.tuit.uz) and on the website of «Ziyonet» Information and educational portal (www.ziyonet.uz.)

Scientific adviser:	**Khamdamov Rustam Khamdamovich** Doctor of Technical Sciences, Professor
Official opponents:	**Bekmuratov Tulkun Fayzievich** Doctor of Technical Sciences, Professor, Academic
	Musaev Mukhammadzhon Makhmudovich Doctor of Technical Sciences, Professor
	Opanasenko Vladimir Nikolaevich Doctor of Technical Sciences, Professor
Leading organization:	**National University of Uzbekistan named after Mirzo Ulugbek**

The defense will take place «30» September 2020 at 15 00 at the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of Tashkent University of Information Technologies (is registered under No. 158). (Address: 100202, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on «18» September 2020 y.
(Dispatching protocol No. 13 on «17» august 2020 y.).

SH.Kh.Fozilov
Deputy Chairman of the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

F.M. Nuraliev
Scientific secretary of scientific council awarding scientific degrees, Doctor of Technical Sciences, Docent

S.K. Ganiev
Chairman of the academic seminar under the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of the dissertation of doctor of science (DSc))

The aim of the research work is the development of adaptive models and methods based on signature and behavioral analysis to protect electronic resources from information security threats.

The object of the research work is the processes of ensuring the security of electronic resources and web applications.

The scientific novelty of the research work is as follows:

created feature space of information security threats to electronic resources on the basis of the international classification of vulnerabilities;

a database of information security threat signatures in electronic resources was created using the object-attribute table;

algorithms for classifying information security threats in electronic resources based on parametric identification methods have been developed;

developed methods of protecting electronic resources from attacks such as SQL injection and XSS using firewall technology for Web applications ;

developed adaptive models for the protection of electronic resources based on signature and behavioral analysis;

methods and algorithms for protecting electronic resources from information security threats have been developed based on language-independent solutions.

Implementation of the research results. Based on the obtained scientific results to ensure the protection of electronic resources from information security threats:

Adaptive models based on signature and behavioral analysis and a software tool developed on their basis have been introduced into the activities of the Center for Information Security and Assistance in Ensuring Public Order(certificate of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan of march 30, 2019 No. 33-8/1922). The use of the results of scientific research made it possible to increase the prompt response to the presence of vulnerabilities in electronic resources by 1.5 times, as well as to increase the security of web resources by 12%.

Methods of ensuring the protection of electronic resources from attacks such as SQL injection and XSS, as well as a mechanism for filtering requests to the Web site, which allows identifying vulnerabilities in electronic resources, and the software developed on their basis were introduced into the activities of the TTT branch of "Uzbektelecom" JSC (certificate of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan of march 30, 2019 No. 33-8/1922). The use of the results of scientific research has made it possible to increase the prompt response to the presence of vulnerabilities in electronic resources by 1.7 times, as well as to increase the security of web resources by 18%.

Algorithms for classifying information security threats in electronic resources based on parametric identification, as well as methods for protecting electronic resources using a firewall for Web applications, and the software developed on their basis have been introduced into the activities of the Directorate for

Information Security and Information Development of "Uzbekistan Temir Yullari" JSC (certificate of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan of march 30, 2019 No. 33-8/1922). The use of the results of scientific research made it possible to increase the response time to the presence of vulnerabilities in electronic resources by 50%, as well as to increase the security of web resources by 50%.

Methods and algorithms for protecting electronic resources from information security threats based on language-independent solutions have been developed, and the software developed on their basis has been introduced into the activities of "SKIF" LLC (certificate of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan of march 30, 2019 No. 33-8/1922). The use of the results of scientific research made it possible to increase the prompt response to the presence of vulnerabilities in electronic resources by 2 times, as well as increase the security of web resources by 30%.

The generated feature space of information security threats in electronic resources, as well as algorithms for classifying information security threats in electronic resources based on parametric identification, and a software tool developed on their basis were introduced into the activities of "SMART SOFTWARE" LLC (certificate of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan of march 30, 2019 No. 33-8/1922). The use of the results of scientific research made it possible to increase the prompt response to the presence of vulnerabilities in electronic resources by 2.5 times, as well as to increase the security of web resources by 50%.

Algorithms and methods for classifying and identifying threats to information security in electronic resources, and the software developed on their basis have been introduced into the activities of "SOFTWARE DESIGN" LLC (certificate of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan of march 30, 2019 No. 33-8/1922). The use of the results of scientific research has made it possible to increase the prompt response to the presence of vulnerabilities in electronic resources by 1.1 times, as well as to increase the security of web resources by 25%.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, five chapters, a conclusion, list of used literature, annexes. The volume of the dissertation is 194 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (I часть; part I)

1. Askar T. Rakhmanov, Rustam Kh. Khamdamov, Komil F. Kerimov, Shukhrat K. Kamalov, Automatic Vulnerability Detection Algorithm for the SQL-Injection// Journal of Automation and Information Sciences DOI: 10.1615/JAutomatInfScien. v51.i6.60 New York, USA 7,2019 P.47-54 (№3; Scopus; IF=0.8).
2. Rustam Kh. Khamdamov, Komil F. Kerimov, Jalol Oybek ugli Ibrahimov, Method of Developing a Web-Application Firewall // Journal of Automation and Information Sciences DOI: 10.1615/JAutomatInfScien.v51.i6.60 New York, USA 6, 2019 P.61-65 (№3; Scopus; IF=0.8).
3. Rustam Kh. Khamdamov, Komil F. Kerimov, Methods of Blocking Vulnerabilities of XSS Type Based on the Service Oriented Architecture // Journal of Automation and Information Sciences DOI: 10.1615/JAutomatInfScien.v51.i12.30 New York, USA 12,2019 P.18-24 (№3; Scopus; IF=0.8).
4. Керимов К.Ф. Адаптивная модель защиты электронных ресурсов от угроз информационной безопасности в электронных ресурсах. // Журнал "Мухаммад ал-Хоразмий авлодлари ". – Ташкент, 2020. – №3(13) – С.3-7. (05.00.00; №10).
5. Рахманов А.Т. Керимов К.Ф., Математический алгоритм обнаружения XSS-атак на WEB-приложения // Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2019. - № 5. – С.84-89. (05.00.00; №5).
6. Рахманов А.Т. , Керимов К.Ф., Камалов Ш.К. "Алгоритм автоматического обнаружения вида SQL инъекции". // Журнал "Мухаммад ал-Хоразмий авлодлари" – Ташкент, 2019. – №2(8) – С.43-47 (05.00.00; №10).
7. Керимов К.Ф., Ибрагимов Ж.О. Методы обхода фильтрации угроз информационной безопасности вида sql инъекции // Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2019. - № 6 – С.79-86. (05.00.00; №5).
8. Керимов К.Ф., Салахутдинов В.Х. Методика оценки риска информационной безопасности электронных ресурсов компьютерной сети при угрозах несанкционированного доступ // Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2018. – № 5–С.84-97. (05.00.00; №5).
9. Керимов К.Ф., Эшметов С.Дж. Методы проектирования и механизмы реализация брандмауэра на основе XML // Узбекский журнал «Проблемы информатики и энергетики». – Ташкент. 2018. - № 4 – С.79-86. (05.00.00; №5).
10. Керимов К.Ф., Камалов Ш.К., Салахутдинов В.Х. Алгоритм оценки критериев принятия решений в задаче управления информационной

системой. // Журнал " Мухаммад ал-Хоразмий авлодлари ". – Ташкент, 2017. – №1(1) – С.19-21 (05.00.00; №10).
11. Керимов К.Ф., Эшметов С.Д, Салахутдинов В.Х. Методика оценки рисков информационной безопасности электронных ресурсов при физических угрозах // Узбекский журнал. «Проблемы информатики и энергетики». – Ташкент, 2017. – № 3 – С.89-96. (05.00.00; №5).
12. Керимов К.Ф., Мухсинов Ш.Ш. Исматуллаев С.О. Брандмауэр баз данных, основанный на обнаружении аномалий. // Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2016. – № 1 – С.89-95. (05.00.00; №5).
13. Керимов К.Ф., Рахматов Ф.А., Аброров Ж.Б. Методы и алгоритмы защиты Web-приложений от общих атак.// Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2016.–№ 2–С.98-105. (05.00.00; №5).
14. Керимов К.Ф., Камалов Ш Исматуллаев С.О. Методы тестирования и защиты Web-приложений от внешних угроз. // «Вестник ТУИТ». – Ташкент, 2016. –№3(39). –С.115-119. (05.00.00; №31).
15. Керимов К.Ф., Хакимов З.Т. Аброров Ж.Б. Методы тестирования Web-приложений на возможность проникновения и взлома. // Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2015. – № 6 – С.72-78. (05.00.00; №5).
16. Керимов К.Ф. Мухсинов Ш.Ш. Исматуллаев С.О. Методы и алгоритмы защиты электронных ресурсов используя брандмауэр для WEB приложений. // «Вестник ТУИТ». – Ташкент, 2015. – № 3 (35) – С.192-195. (05.00.00; №31).
17. Керимов К.Ф., Мухсинов Ш.Ш. Формирование признаков угроз информационной безопасности электронного ресурса. // Узбекский журнал «Проблемы информатики и энергетики». - Ташкент, 2014. – № 3–4, – С. 112–116. (05.00.00; №5).
18. Керимов К.Ф., Мухсинов Ш.Ш. Методы и алгоритмы защиты электронной почты от спам-сообщений // «Вестник ТУИТ». – Ташкент, 2014. – № 29. – С.53-56. (05.00.00; №31).

II бўлим (II часть; part II)

19. Хамдамов Р.Х., Керимов К.Ф., Ибрагимов Дж.О. Методика разработки брандмауэра веб-приложений // Международный научно-технический журнал "Проблемы управления и информатики". – Украина, Киев 2019. – №3. С.105-110.
20. Хамдамов Р.Х., Керимов К.Ф., Методы блокирования уязвимостей вида XSS на основе сервис ориентированной архитектуры // Международный научно-технический журнал "Проблемы управления и информатики". – Украина, Киев 2019. – №6. – С.86-91.
21. Рахманов А.Т., Хамдамов Р.Х., Керимов К.Ф., Камалов Ш.К. Алгоритм автоматического обнаружения уязвимости вида SQL инъекции. XII

международная научно-практическая конференция «Компьютерные системы и сетевые технологии» (CSNT-2019), Украина, Киев, 2019. –с.100-101.
22. Хамдамов Р.Х., Керимов К.Ф., Камалов Ш.К. Методы блокирования уязвимостей вида XSS на основе сервис ориентированной архитектуры. XII международная научно-практическая конференция «Компьютерные системы и сетевые технологии» (CSNT-2019), –Украина, Киев, 2019. – С.119-120.
23. Хамдамов Р.Х., Керимов К.Ф. Методы блокирования уязвимостей вида XSS на основе сервис ориентированной архитектуры. Доклады Республиканской научно-технической конференции «Современное состояние и перспективы применения информационных технологий в управлении». – Самарканд, 2019. – С.417-419
24. Хамдамов Р.Х., Керимов К.Ф. Математический метод обнаружения XSS атак на web приложения. Доклады Республиканской научно-технической конференции «Современное состояние и перспективы применения информационных технологий в управлении». – Самарканд, 2019. – С.419-422
25. Керимов К.Ф., Латипова Н.Х., Мухсинов Ш.Ш. Алгоритм классификации угроз информационной безопасности в электронных ресурсах. // VII Международная научная конференция «Приоритетные направления в области науки и технологии в XXI веке». Ташкент- 2014. № 3. С.273-275
26. Керимов К.Ф. Камалов Ш.К., Толипов Д. Агентство по интеллектуальной собственности РУз. Свидетельство об официальной регистрации программы для электронно-вычислительных машин // DGU 05916 г. Ташкент. 26.12.2018 «Биометрическая система контроля доступа Biocontrol»
27. Керимов К.Ф., Камалов. Ш.К. "Adaptive web protector" Агентство по интеллектуальной собственности РУз. Свидетельство об официальной регистрации программы для электронно-вычислительных машин №DGU 05805 г. Ташкент 27.11.2018
28. Керимов К.Ф., Камалов Ш.К. "Web vulnerabilities scanner" // Агентство по интеллектуальной собственности РУз. Свидетельство об официальной регистрации программы для электронно-вычислительных машин № DGU 03977 г. Ташкент 20.09.2016
29. Керимов К.Ф., Камалов Ш. WEB defender // Агентство по интеллектуальной собственности РУз. Свидетельство об официальной регистрации программы для электронно-вычислительных машин № DGU 03978 г. Ташкент 20.09.2016.

Автореферат «Информатика ва энергетика муаммолари» журнали таҳририяти таҳриридан ўтказилди ва ўзбек, рус тилларидаги матнларини мослиги текширилди.